Nessus 5.0 Guia de instalação e configuração

30 de novembro de 2012

(Revisão 16)

Índice

Introdução 4
Padrões e convenções 4
Organização 4
O que há de novo no Nessus 5 4
Atualizações dos recursos básicos 4
Navegação 5
Análise 5
Relatórios 5
Nova GUI (interface do usuário) do servidor 5
Sistemas operacionais compatíveis 5
Conceitos básicos 6
Pré-requisitos 7
Nessus Unix 7
Nessus para Windows 7
Opções de instalação 8
Firewalls instalados no host 8
Inscrições em plugins de vulnerabilidades 8
Tipos de inscrições 8
Suporte para IPv6 9
Unix/Linux 9
Atualizações 9
Instalação 13
Como iniciar o daemon do Nessus 15
Como parar o daemon do Nessus 16
Remoção do Nessus 17
Windows 20
Atualizações 20
Atualização do Nessus 4.x 20
Atualização do Nessus 3.x 21
Instalação 21
Download do Nessus 21
Instalação 21
Problemas de instalação 22
Iniciar e parar o Daemon Nessus 25
Remoção do Nessus 26
Mac OS X 26
Atualizações 26
Instalação 26
Problemas de instalação 27
Iniciar e parar o serviço Nessus 30
Remoção do Nessus 30
Registro de feed e configuração da GUI (interface do usuário) 31

Configuração 37
Configurações de proxy da Web 37
Redefinir códigos de ativação e atualizações off-line 39
Opções de configuração avançadas 39
Criação e gerenciamento de usuários do Nessus 40
Configuração do daemon do Nessus (usuários avançados) 43
Opções de configuração 44
Configuração do Nessus com certificado SSL personalizado 47
Autenticação do Nessus com certificado SSL 48
Autenticação de certificado de cliente SSL 48
Configurar o Nessus para certificados 48
Criar certificados SSL do Nessus para login 49
Ativar conexões com cartão inteligente ou cartão CAC 50
Conexão com certificado ou navegador ativado com cartão 52
Nessus sem acesso à Internet 53
Como gerar um código de confirmação 53
Como obter e instalar plugins atualizados 53
Como usar e gerenciar o Nessus a partir da linha de comando 56
Diretórios principais do Nessus 56
Como criar e gerenciar usuários do Nessus com limitações de conta 56
Opções de linha de comando do Nessusd 57
Manipulação do serviço Nessus por meio de CLI do Windows 59
Como trabalhar como SecurityCenter 59
Descrição do SecurityCenter 59
Configuração do SecurityCenter 4.0-4.2 para funcionar com o Nessus 59
Configuração do SecurityCenter 4.4 para funcionar com o Nessus 60
Firewalls instalados no host 61
Solução de problemas do Nessus para Windows 62
Problemas de instalação/atualização 62
Problemas de varredura 62
Para obter mais informações 64
Declarações de licença de terceiros 65
Sobre a Tenable Network Security 68

Introdução

Este documento descreve a instalação e a configuração de scanner do vulnerabilidades **Nessus 5,0** da Tenable Network Security. Envie seus comentários e sugestões para o e-mail support@tenable.com.

A Tenable Network Security, Inc. desenvolveu e produziu o scanner de vulnerabilidades Nessus. Além de aprimorar constantemente o motor de detecção do Nessus, a Tenable cria a maioria dos plugins disponíveis para o scanner, além de verificações de conformidade e uma grande variedade de políticas de auditoria.

Os pré-requisitos, opções de implementação e orientações de instalação serão descritos neste documento. O leitor deve ter conhecimentos básicos sobre Unix e varreduras de vulnerabilidades.

Padrões e convenções

Este documento é a tradução de uma versão original em inglês. Algumas partes do texto permanecem em inglês para indicar a representação do próprio produto.

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **`courier bold`**, por exemplo: **`setup.exe.`**

As opções de linha de comando e palavras-chaves também são impressas indicadas com a fonte **`courier bold`**. Os exemplos de linhas de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Os exemplos de linhas de comando exibirão o comando executado em **`courier bold`** para indicar o que o usuário digitou, enquanto que o exemplo de saída gerado pelo sistema será indicado em `courier` (sem negrito). Um exemplo da execução do comando **`pwd`** do Unix é apresentado a seguir:

```
# pwd
/opt/nessus/
#
```

As observações e considerações importantes são destacadas com este símbolo nas caixas de texto escurecidas.

As dicas, exemplos e práticas recomendados são destacados com este símbolo em branco sobre fundo azul.

Organização

Como a GUI (interface do usuário) Nessus é padronizada, independentemente do sistema operacional, este documento apresenta as informações específicas do sistema operacional primeiro e, em seguida, a funcionalidade que é comum a todos os sistemas operacionais.

O que há de novo no Nessus 5

Com o lançamento do Nessus 5, a configuração de gerenciamento do usuário e do servidor Nessus (daemon) é controlada pela GUI (interface do usuário) Nessus e não pelo NessusClient independente ou arquivo **`nessusd.conf`**. **A GUI (interface do usuário) Nessus é uma interface baseada na Web que permite controlar a configuração, criação de políticas, verificações e todos os relatórios.**

Atualizações dos recursos básicos

A lista a seguir contém alguns dos novos recursos disponíveis no Nessus 5. Para obter uma lista completa das alterações, consulte as notas da versão no Fórum de discussão.

Navegação

- Novo painel de resumo do host: Com os painéis de resumo do host e de resumo de vulnerabilidades, ficou mais fácil visualizar o nível de risco sem executar um relatório.
- As barras gráficas mostram instantaneamente os hosts mais vulneráveis.

Análise

- Nessus 5 agora possui cinco níveis de gravidade: informativo, baixo risco, médio risco, alto risco e crítico.
- Os usuários podem selecionar vários critérios de filtragem, como data de publicação da vulnerabilidade, ID do banco de dados da vulnerabilidade (por exemplo: CVE, OSVDB, Bugtraq ID, CERT, Secunia), tipo de plugin (local ou remoto), Information Assurance Vulnerability Alert (IAVA), entre outros.
- recurso “Audit trail” (Trilha de auditoria) registra por que uma vulnerabilidade NÃO aparece no relatório para um determinado host.

Relatórios

- Sistema de relatórios com base em capítulos, organizados entre vulnerabilidades e conformidade.
- Os relatórios podem ser gerados em formatos nativos do Nessus, HTML e, atualmente, formatos PDF (requer que o Oracle Java esteja instalado no servidor Nessus).

Nova GUI (interface do usuário) do servidor

- A interface baseada na Web controla a configuração e gerenciamento de usuários, além de criação de políticas, verificações e todos os relatórios.
- As atualizações de plugin podem ser iniciadas na interface baseada na Web.
- Nessus Web Server é compatível com IPv6.

Sistemas operacionais compatíveis

O Nessus está disponível e funciona com vários sistemas operacionais e plataformas:

- Debian 6 (i386 e x86-64)
- Fedora Core 16 (i386 e x86-64)
- FreeBSD 9 (i386 e x86-64)
- Mac OS X 10.6 e 10.7 (i386 e x86-64)
- Red Hat ES 4 / CentOS 4 (i386)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 e x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 e x86-64) [Servidor, Desktop, Estação de trabalho]
- SuSE 10 (x86-64), 11 (i386 e x86-64)
- Ubuntu 8.04, 9.10, 10.04, 10.10, 11.10 e 12.04 (i386 e x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2 *, Vista e 7 (i386 e x86-64)

Observe que, no Windows Server 2008 R2, a versão integrada do Microsoft IE não possui interface com a instalação do Java corretamente. Isso faz com o que o Nessus não funcione conforme o esperado em algumas situações. Além disso, a política da Microsoft não recomenda o uso de MSIE em sistemas operacionais de servidor. A Tenable recomenda que o registro e as atividades de verificação sejam realizados em um sistema desktop.

Conceitos básicos

A Nessus é um scanner de segurança de rede poderoso e fácil de usar, com um banco de dados de plugins abrangente e atualizado diariamente. Atualmente, é considerado um dos principais produtos do seu gênero em todo o setor de segurança e conta com o apoio de organizações profissionais de segurança da informação, como o Instituto SANS. O Nessus permite realizar auditorias remotas e determinar se a rede foi comprometida ou usada de maneira indevida. O Nessus também permite verificar a presença de vulnerabilidades, especificações de conformidade, violações de políticas de conteúdo e outras anomalias em um computador local.

- **Varredura inteligente –** Ao contrário de outros scanners de segurança, o Nessus não gera alarmes falsos. O programa não pressupõe que um determinado serviço está sendo executado em uma porta fixa. Isso significa que, se o servidor Web for executado na porta 1234, o Nessus o detectará e testará sua segurança da forma apropriada. O programa verificará uma vulnerabilidade por meio de exploração sempre que possível. Nos casos em que isso não for confiável ou afetar negativamente o alvo, o Nessus conta com um banner de servidor para determinar a presença da vulnerabilidade. Nesse caso, o relatório gerado indicará se esse método foi utilizado.

- **Arquitetura modular –** A arquitetura cliente/servidor oferece a flexibilidade de instalar o scanner (servidor) e conectar-se à GUI (interface gráfica do usuário) (cliente) por intermédio de qualquer computador com um navegador, reduzindo assim os custos de gerenciamento (um servidor pode ser acessado por vários clientes).

- **Compatível com CVE –** A maioria dos plugins se conecta ao CVE para que os administradores possam recuperar mais informações sobre vulnerabilidades publicadas. As referências ao Bugtraq (BID), OSVDB e alertas de segurança dos fornecedores também são incorporadas com frequência.

- **Arquitetura de plugin –** Os testes de segurança são gerados por meio de um plugin externo e agrupado em uma das 42 famílias. Dessa forma, é possível adicionar facilmente seus próprios testes, selecionar plugins específicos ou escolher uma família inteira sem a necessidade de leitura do código do mecanismo do servidor Nessus, **`nessusd`**. A lista completa dos plugins do Nessus está disponível em http://www.nessus.org/plugins/index.php?view=all.

- **NASL –** O scanner Nessus utiliza NASL (Nessus Attack Scripting Language), uma linguagem criada especificamente para a criação de testes de segurança de maneira fácil e rápida.

- **Banco de dados de vulnerabilidades de segurança atualizado –** A Tenable dedica-se a desenvolver verificações de segurança para vulnerabilidades emergentes. Nosso banco de dados de verificações de segurança é atualizado diariamente e todas as verificações de segurança mais recentes estão disponíveis no link http://www.nessus.org/scripts.php.

- **Teste simultâneo de hosts –** Dependendo da configuração do sistema de scanner Nessus, é possível auditar um grande número de hosts ao mesmo tempo.

- **Reconhecimento inteligente do serviço –** O Nessus reconhece quando os hosts de destino não são compatíveis os números de portas atribuídos pelo IANA. Isso significa que ele reconhecerá um servidor de FTP funcionando em uma porta que não seja padrão (por exemplo: 31337) ou um servidor de Web funcionando na porta 8080 em vez da porta 80.

- **Vários serviços –** Se dois ou mais servidores de Web forem executados em um host (por exemplo: um na porta 80 e outro na porta 8080), o Nessus identificará e testará todos eles.

- **Compatibilidade entre plugins –** Os testes de segurança realizados pelos plugins do Nessus impedem que sejam realizadas verificações desnecessárias. Se o servidor de FTP não permitir logins anônimos, não serão realizadas verificações de segurança relacionadas a logins anônimos.
- **Relatórios completos –** Além de detectar as vulnerabilidades de segurança existentes na rede e o nível de risco de cada uma delas (baixo, médio, alto e grave), o Nessus oferece soluções de como atenuá-las.
- **Suporte total a SSL –** O Nessus é capaz de testar os serviços oferecidos por SSL, como HTTPS, SMTPS, IMAPS entre outros.
- **Smart Plugins (opcional) –** O Nessus tem uma opção "optimization" (otimização), que determinará quais plugins devem ou não ser aplicados ao host remoto. Por exemplo: o Nessus não verificará vulnerabilidades de sendmail no Postfix.
- **Testes não destrutivos (opcional) –** Determinadas verificações podem ser prejudiciais a alguns serviços de rede. Caso não queira correr o risco de causar uma falha de serviço na sua rede, ative a opção “safe checks” (verificações segura) do Nessus. Esse comando fará com que o Nessus use banners em vez de explorar falhas reais para detectar uma vulnerabilidade.
- **Fórum aberto –** Encontrou um erro? Dúvidas sobre o Nessus? Inicie uma discussão em https://discussions.nessus.org/.

Pré-requisitos

A Tenable recomenda, no mínimo, 2 GB de memória para o funcionamento correto do Nessus. Para varreduras maiores em várias redes, recomendam-se pelo menos 3 GB de memória, mas podem ser necessários até 4 GB para maior capacidade, que inclui trilhas de auditoria e geração de relatórios em PDF.

Recomenda-se um processador Pentium 3 operando a 2 GHz ou mais. Para usar o Mac OS X, recomenda-se um processador Intel® Dual Core operando a 2 GHz ou mais. É recomendável a instalação do Nessus em sistemas de 64 bits. O sistema deve ter, no mínimo, 30 GB de espaço livre em disco para o Nessus e para os dados de varredura subsequentes.

O Nessus pode funcionar em uma instância do VMware. No entanto, se a máquina virtual usar a conversão de endereços de rede (NAT) para acessar a rede, diversas verificações de vulnerabilidade do Nessus, a enumeração de hosts e a identificação de sistemas operacionais serão afetadas negativamente.

Nessus Unix

Antes de instalar o Nessus no Unix/Linux, são necessárias várias bibliotecas. Normalmente, elas acompanham a maioria dos sistemas operacionais e dispensam uma instalação separada.

- zlib
- Biblioteca GNU C (por exemplo: libc)
- Oracle Java (apenas para relatórios em PDF)

O Java deve estar instalado no host antes da instalação do Nessus. Se o Java for instalado posteriormente, o Nessus deverá ser reinstalado.

Nessus para Windows

As atualizações feitas pela Microsoft no Windows XP SP2 e nas versões mais recentes podem afetar o desempenho do Nessus para Windows. Para aumentar a velocidade e a confiabilidade das varreduras, é recomendável que o Nessus para Windows seja instalado em um produto de servidor da família Microsoft Windows, como o Windows Server 2003. Para obter mais informações, consulte a seção “Solução de Problemas do Nessus para Windows”.

Opções de instalação

Ao instalar o Nessus, muitas vezes é necessário ter conhecimentos de roteamento, filtros e políticas de firewall. Recomenda-se que o Nessus seja instalado de modo que a conectividade IP com as redes a serem examinadas não seja prejudicada. A instalação em um dispositivo NAT não é desejável, a menos que a varredura seja realizada na rede interna. Sempre que a verificação de vulnerabilidade for direcionada a um NAT ou proxy de aplicativos, a verificação pode ser distorcida e gerar um falso positivo ou negativo. Além disso, se o sistema no qual o Nessus está instalado tiver firewalls no computador, as ferramentas podem limitar a eficácia de uma varredura remota de vulnerabilidades.

Os firewalls de host podem interferir na varredura de vulnerabilidades de rede. Dependendo da configuração do firewall, pode impedir, gerar falsos negativos ou ocultar as sondas de uma varredura do Nessus.

Alguns dispositivos de rede que realizam a inspeção dinâmica (stateful inspection), como firewalls, balanceadores de carga e sistemas de detecção/prevenção de intrusões, podem reagir negativamente quando uma varredura for realizada através deles. O Nessus possui várias opções de configuração que podem ajudar a reduzir o impacto da varredura por meio desses dispositivos, no entanto, a melhor maneira de prevenir os problemas inerentes à varredura com esses dispositivos de rede é realizar uma varredura credenciada.

Firewalls instalados no host

Se o servidor Nessus estiver configurado em um host com um firewall “pessoal”, como ZoneAlarm, Sygate, firewall do Windows ou qualquer outro software de firewall, será necessário que as conexões sejam permitidas a partir do endereço IP do cliente Nessus.

Normalmente, a porta 8834 é usada para o Nessus Web Server (interface do usuário). Nos sistemas Microsoft XP Service Pack 2 (SP2) e posteriores, clique em “**Security Center**” (Central de Segurança) no “**Control Panel**” (Painel de Controle) para gerenciar as configurações da opção “Windows Firewall” (Firewall do Windows). Para abrir a porta 8834, selecione a guia “**Exceptions**” (Exceções) e adicione a porta “8834” à lista.

Para outros softwares de firewall pessoal, consulte a documentação para obter instruções de configuração.

Inscrições em plugins de vulnerabilidades

Um grande número de vulnerabilidades emergentes é divulgado por fornecedores, pesquisadores e outras fontes todos os dias. A Tenable se esforça para testar e disponibilizar o mais rapidamente possível as verificações de vulnerabilidades publicadas recentemente, normalmente 24 horas após a divulgação. A verificação de uma vulnerabilidade específica é conhecida pelo scanner Nessus como um “plugin”. A lista completa de todos os plugins do Nessus está disponível em http://www.nessus.org/plugins/index.php?view=all. A Tenable distribui os plugins de vulnerabilidade mais recentes para o Nessus de duas maneiras: ProfessionalFeed e HomeFeed.

Os plugins são baixados diretamente da Tenable por meio de um processo automatizado do Nessus. O Nessus verifica as assinaturas digitais de todos os plugins baixados para garantir a integridade dos arquivos. Nas instalações do Nessus sem acesso à Internet, pode ser usado um processo de atualização offline para garantir que o scanner permaneça atualizado.

O usuário deve se registrar para obter um feed de plugin e atualizá-los antes de iniciar o Nessus e a interface de varredura do Nessus se torne disponível. A atualização do plugin ocorre em segundo plano após o registro inicial do scanner e pode levar vários minutos.

Tipos de inscrições

A Tenable presta suporte comercial aos clientes do ProfessionalFeed e usuários do Nessus 5 por meio do Tenable Support Portal ou por e-mail. O ProfessionalFeed também contém um conjunto de verificações de conformidade de host para Unix e Windows, que permitem realizar auditorias de conformidade, como SOX, FISMA ou PCI DSS.

É possível adquirir um ProfessionalFeed na Loja Online da Tenable (https://store.tenable.com/) ou por meio de uma ordem de compra enviada aos Authorized ProfessionalFeed Partners. O usuário receberá um Activtion Code (Código de Ativação) da Tenable. Esse código será usado para configurar a cópia do Nessus para atualizações.

Se o Nessus for usado junto com o SecurityCenter da Tenable, o SecurityCenter terá acesso ao ProfessionalFeed e atualizará automaticamente os scanners Nessus.

Se o usuário for uma organização beneficente de acordo com 501(c)(3), terá o direito de solicitar o ProfessionalFeed sem custos. Para obter mais informações, visite a página Tenable Charitable Organization Subscription Program.

Se o Nessus for instalado para uso doméstico e não profissional, o usuário deve se inscrever no HomeFeed. O uso do HomeFeeds é gratuito, mas há uma licença separada do HomeFeed cujos termos e condições os usuários devem aceitar.

Suporte para IPv6

O Nessus oferece suporte para varredura de recursos baseados em IPv6. Vários sistemas operacionais e dispositivos são distribuídos atualmente com suporte para IPv6. Para realizar varreduras de recursos com IPv6, pelo menos uma interface IPv6 deve ser configurada no computador em que o Nessus estiver instalado e o Nessus deve estar em uma rede que reconheça o IPv6 (o Nessus não pode examinar recursos IPv6 através do IPv4, mas pode enumerar as interfaces IPv6 através de varreduras credenciadas por IPv4). A notação IPv6 completa e compactada é reconhecida para iniciar varreduras.

O Microsoft Windows não possui algumas das principais APIs necessárias para a falsificação de pacotes IPv6 (por exemplo: obtenção do endereço MAC do roteador, tabela de roteamento etc.). Isto impede que o scanner de portas funcione corretamente. A Tenable está desenvolvendo aprimoramentos que solucionem as restrições de API em futuras versões do Nessus. Até agora, o suporte IPv6 estava disponível apenas em plataformas *nix.

Unix/Linux

Atualizações

Esta seção descreve como atualizar o Nessus a partir de uma versão de instalação anterior do programa.

A tabela a seguir apresenta instruções de atualização do servidor Nessus em todas as plataformas suportadas anteriormente. Os parâmetros de configuração e os usuários criados anteriormente permanecerão intactos.

Antes de interromper o **nessusd**, verifique se todas as varreduras em execução foram concluídas.

Todas as instruções especiais de atualização são indicadas em uma observação após o exemplo.

Plataforma	Instruções de atualização
Red Hat ES 4 e CentOS 4 (32 bits); Red Hat ES 5, CentOS 5 e Oracle Linux 5 (32 e 64 bits); Red Hat ES 6, CentOS 6 e Oracle Linux 6 (32 e 64 bits)	

Comandos de atualização	`# service nessusd stop`
	
	Use um dos comandos abaixo correspondente à versão do Red Hat que está em uso:
	
	`# rpm -Uvh Nessus-5.0.1-es4.i386.rpm`
	`# rpm -Uvh Nessus-5.0.1-es5.i386.rpm`
	`# rpm -Uvh Nessus-5.0.1-es5.x86_64.rpm`
	`# rpm -Uvh Nessus-5.0.1-es6.i686.rpm`

	`# rpm -Uvh Nessus-5.0.1-es6.x86_64.rpm`
	
	Quando a atualização for concluída, reinicie o serviço **nessusd** com o seguinte comando:
	
	`# service nessusd start`

Exemplo de resultado	`# service nessusd stop`
	`Shutting down Nessus services: [ OK ]`
	`# rpm -Uvh Nessus-5.0.1-es5.i386.rpm`
	`Preparing...`
	`########################################### [100%]`
	`Shutting down Nessus services: /etc/init.d/nessusd: … 1:Nessus`
	`########################################### [100%]`
	`Fetching the newest plugins from nessus.org...`
	`Fetching the newest updates from nessus.org...`
	`Done. The Nessus server will start processing these plugins within a minute`
	`nessusd (Nessus) 5.0.1 [build R23016] for Linux`
	`(C) 1998 - 2012 Tenable Network Security, Inc.`
	
	`Processing the Nessus plugins...`
	`[##################################################]`
	
	`All plugins loaded`
	`- You can start nessusd by typing /sbin/service nessusd start`
	`- Then go to https://localhost:8834/ to configure your scanner# service nessusd start`
	`Starting Nessus services: [ OK ]`
	`#`

Fedora Core 16 (32 e 64 bits)	

Comandos de atualização	`# service nessusd stop`
	
	Use um dos comandos abaixo correspondente à versão do Fedora Core que está em uso:
	
	`# rpm -Uvh Nessus-5.0.1-fc16.i686.rpm`
	`# rpm -Uvh Nessus-5.0.1-fc16.x86_64.rpm`
	
	Quando a atualização for concluída, reinicie o serviço nessusd com o seguinte comando:
	
	`# service nessusd start`

Exemplo de resultado	`# service nessusd stop`
	`Shutting down Nessus services: [ OK ]`
	`# rpm -Uvh Nessus-5.0.1-fc16.i386.rpm`
	
	`[..]`
	
	`# service nessusd start`
	`Starting Nessus services: [ OK ]`
	`#`

SuSE 10 (64 bits), 11 (32 e 64 bits)	

Comandos de atualização	`# service nessusd stop`
	
	Use um dos comandos abaixo correspondente à versão do SuSE que está em uso:
	
	`# rpm -Uvh Nessus-5.0.1-suse10.x86_64.rpm`
	`# rpm -Uvh Nessus-5.0.1-suse11.i586.rpm`
	`# rpm -Uvh Nessus-5.0.1-suse11.x86_64.rpm`
	
	Quando a atualização for concluída, reinicie o serviço **nessusd** com o seguinte comando:
	
	`# service nessusd start`

Exemplo de resultado	`# service nessusd stop`
	`Shutting down Nessus services: [ OK ]`
	`# rpm -Uvh Nessus-5.0.1-suse11.i586.rpm`
	`Preparing...`
	
	`[..]`
	
	`# service nessusd start`
	`Starting Nessus services: [ OK ]`
	`#`

Debian 6 (32 e 64 bits)	

Comandos de atualização	`# /etc/init.d/nessusd stop`
	
	Use um dos comandos abaixo correspondente à versão do Debian que está em uso:
	
	`# dpkg -i Nessus-5.0.1-debian6_i386.deb`
	`# dpkg -i Nessus-5.0.1-debian6_amd64.deb`
	
	`# /etc/init.d/nessusd start`

Exemplo de resultado	`# /etc/init.d/nessusd stop`
	
	`# dpkg -i Nessus-5.0.1-debian6_i386.deb`
	`(Reading database ... 19831 files and directories currently installed.)`
	`Preparing to replace nessus 4.4.0 (using Nessus-5.0.1-debian6_i386.deb) ...`
	
	`[..]`
	
	`# /etc/init.d/nessusd start`
	
	`Starting Nessus : .`
	`#`

Ubuntu 8.04, 9.10, 10.04, 10.10 e 11.10 (32 e 64 bits)	
Comandos de atualização	`# /etc/init.d/nessusd stop`

	Use um dos comandos abaixo correspondente à versão do Ubuntu que está em uso: **# dpkg -i Nessus-5.0.1-ubuntu804_i386.deb** **# dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb** **# dpkg -i Nessus-5.0.1-ubuntu910_i386.deb** **# dpkg -i Nessus-5.0.1-ubuntu910_amd64.deb** **# dpkg -i Nessus-5.0.1-ubuntu1010_i386.deb** **# dpkg -i Nessus-5.0.1-ubuntu1010_amd64.deb** **# dpkg -i Nessus-5.0.1-ubuntu1110_i386.deb** **# dpkg -i Nessus-5.0.1-ubuntu1110_amd64.deb** **# /etc/init.d/nessusd start**
Exemplo de resultado	**# /etc/init.d/nessusd stop** **# dpkg -i Nessus-5.0.1-ubuntu804_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 4.4.0 (using Nessus-5.0.0-ubuntu810_i386.deb) ... [..] **# /etc/init.d/nessusd start** Starting Nessus : . #
FreeBSD 9 (32 e 64 bits)	
Comandos de atualização	**# killall nessusd** **# pkg_info** Este comando gera uma lista de todos os pacotes instalados, e suas descrições. O exemplo a seguir descreve o resultado do comando anterior exibindo o pacote do Nessus: Nessus-4.4.4 A powerful security scanner Exclua o pacote do Nessus por meio do seguinte comando: **# pkg_delete <package name>** Use um dos comandos abaixo correspondente à versão do FreeBSD que está em uso: **# pkg_add Nessus-5.0.1-fbsd9.tbz** **# pkg_add Nessus-5.0.1-fbsd9.amd64.tbz** **# /usr/local/nessus/sbin/nessusd -D**
Exemplo de resultado	**# killall nessusd** **# pkg_delete Nessus-4.4.4** **# pkg_add Nessus-5.0.1-fbsd9.tbz** nessusd (Nessus) 5.0.1. for FreeBSD (C) 2011 Tenable Network Security, Inc.

	[..] # **/usr/local/nessus/sbin/nessusd -D** nessusd (Nessus) 5.0.1. for FreeBSD (C) 2011 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded #
Observações	Para atualizar o Nessus no FreeBSD, é preciso desinstalar primeiro a versão existente e instalar a versão mais recente. Este processo não excluirá os arquivos de configuração ou os arquivos que não faziam parte da instalação original.

Instalação

Baixe a última versão do Nessus em http://www.nessus.org/products/nessus/nessus-download-agreement ou por meio do Tenable Support Portal. Verifique a integridade do pacote de instalação ao comparar o checksum MD5 do download com o checksum MD5 listado no arquivo **MD5.asc** aqui.

Exceto quando indicado em contrário, todos os comandos devem ser executados como usuário root do sistema. Em geral, as contas comuns de usuários não possuem os privilégios necessários para instalar este software.

A tabela a seguir apresenta instruções de instalação do servidor Nessus em todas as plataformas suportadas. Todas as instruções especiais de atualização são indicadas em uma observação após o exemplo.

Plataforma	Instruções de instalação
Red Hat ES 4 e CentOS 4 (32 bits); Red Hat ES 5, CentOS 5 e Oracle Linux 5 (32 e 64 bits); Red Hat ES 6, CentOS 6 e Oracle Linux 6 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do Red Hat que está em uso: # **rpm -ivh Nessus-5.0.1-es4.i386.rpm** # **rpm -ivh Nessus-5.0.1-es5.i386.rpm** # **rpm -ivh Nessus-5.0.1-es5.x86_64.rpm** # **rpm -ivh Nessus-5.0.1-es6.i686.rpm** # **rpm -ivh Nessus-5.0.1-es6.x86_64.rpm**
Exemplo de resultado	# **rpm -ivh Nessus-5.0.1-es4.i386.rpm** Preparing... ### [100%] 1:Nessus ### [100%] nessusd (Nessus) 5.0.1 [build R23011] for Linux (C) 1998 - 2012 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded

	- You can start nessusd by typing /sbin/service nessusd start - Then go to https://squirrel:8834/ to configure your scanner #
Fedora Core 16 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do Fedora Core que está em uso: # **rpm -ivh Nessus-5.0.1-fc16.i686.rpm** # **rpm -ivh Nessus-5.0.1-fc16.x86_64.rpm**
Exemplo de resultado	# **rpm -ivh Nessus-5.0.1-fc16.i386.rpm** Preparing... [..] #
SuSE 10 (64 bits), 11 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do SuSE que está em uso: # **rpm –ivh Nessus-5.0.1-suse10.x86_64.rpm** # **rpm –ivh Nessus-5.0.1-suse11.i586.rpm** # **rpm –ivh Nessus-5.0.1-suse11.x86_64.rpm**
Exemplo de resultado	# **rpm -ivh Nessus-5.0.1-suse11.i586.rpm** Preparing... ## [100%] 1:Nessus ## [100%] [..] #
Debian 6 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do Debian que está em uso: # **dpkg -i Nessus-5.0.1 –debian6_i386.deb** # **dpkg -i Nessus-5.0.1 –debian6_amd64.deb**
Exemplo de resultado	# **dpkg -i Nessus-5.0.1-debian6_i386.deb** Selecting previously deselected package nessus. (Reading database ... 36954 files and directories currently installed.) Unpacking nessus (from Nessus-5.0.1-debian6_i386.deb) ... Setting up nessus (5.0.1) ... [..] #
Ubuntu 8.04, 9.10, 10.04, 10.10 e 11.10 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do Ubuntu que está em uso:

	# **dpkg -i Nessus-5.0.1-ubuntu804_i386.deb** # **dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb** # **dpkg -i Nessus-5.0.1-ubuntu910_i386.deb** # **dpkg -i Nessus-5.0.1-ubuntu910_amd64.deb** # **dpkg -i Nessus-5.0.1-ubuntu1010_i386.deb** # **dpkg -i Nessus-5.0.1-ubuntu1010_amd64.deb** # **dpkg -i Nessus-5.0.1-ubuntu1110_i386.deb** # **dpkg -i Nessus-5.0.1-ubuntu1110_amd64.deb**
Exemplo de resultado	# **dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb** Selecting previously deselected package nessus. (Reading database ... 32444 files and directories currently installed.) Unpacking nessus (from Nessus-5.0.1-ubuntu804_amd64.deb) ... Setting up nessus (5.0.1) ... [..] #
FreeBSD 9 (32 e 64 bits)	
Comando de instalação	Use um dos comandos abaixo correspondente à versão do FreeBSD que está em uso: # **pkg_add Nessus-5.0.1-fbsd9.tbz** # **pkg_add Nessus-5.0.1-fbsd9.amd64.tbz**
Exemplo de resultado	# **pkg_add Nessus-5.0.1-fbsd9.tbz** nessusd (Nessus) 5.0.1 for FreeBSD (C) 1998 - 2012 Tenable Network Security, Inc. [..] #

Após o término da instalação, inicie o daemon **nessusd** conforme as instruções na seção seguinte, dependendo da distribuição. Depois de o Nessus ser instalado, visite a URL do scanner fornecido para completar o processo de registro.

Nota: As instalações em ambiente Unix podem gerar um URL com um nome de host correspondente que não está no DNS (por exemplo: http://mybox:8834/). Se o nome não estiver no DNS, será preciso se conectar ao servidor Nessus com um endereço IP ou nome DNS válido.

Depois de concluir o processo, é recomendável autenticar e personalizar as opções de configuração para o seu ambiente, conforme descrito na seção "Registro de feed e configuração da GUI (interface do usuário)".

O Nessus deve ser instalado em **/opt/nessus**. No entanto, se **/opt/nessus** for um **symlink**apontando para outro lugar, ele será aceito.

Como iniciar o daemon do Nessus

Inicie o serviço Nessus como root com o seguinte comando:

Linux e Solaris:

```
# /opt/nessus/sbin/nessus-service -D
```

FreeBSD:
```
# /usr/local/nessus/sbin/nessus-service -D
```

O exemplo a seguir mostra uma tela de inicialização do **nessusd** no Red Hat:

```
[root@squirrel ~]# /sbin/service nessusd start
Starting Nessus services:                                  [  OK  ]
[root@squirrel ~]#
```

Para suprimir o resultado do comando, use a opção "-q" da seguinte forma:

Linux e Solaris:
```
# /opt/nessus/sbin/nessus-service -q -D
```

FreeBSD:
```
# /usr/local/nessus/sbin/nessus-service -q -D
```

O Nessus também pode ser iniciado com o comando a seguir, dependendo da plataforma de sistema operacional:

Sistema operacional	Comando para iniciar o nessusd
Red Hat, CentOS e Oracle Linux	`# /sbin/service nessusd start`
Fedora Core	`# /sbin/service nessusd start`
SuSE	`# /etc/rc.d/nessusd start`
Debian	`# /etc/init.d/nessusd start`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh start`
Solaris	`# /etc/init.d/nessusd start`
Ubuntu	`# /etc/init.d/nessusd start`

Continue na seção "Registro de feed e configuração da GUI (interface do usuário)" para instalar o plugin do Activtion Code (Código de Ativação).

Como parar o daemon do Nessus

Caso seja necessário parar o serviço **nessusd** por qualquer motivo, o comando a seguir interromperá o Nessus e todas as varreduras em andamento:

```
# killall nessusd
```

Em vez disso, recomendamos que os scripts de desligamento gradual fornecidos pelo sistema operacional sejam usados:

Sistema operacional	Comando de interrupção do nessusd
Red Hat, CentOS e Oracle Linux	`# /sbin/service nessusd stop`
Fedora Core	`# /sbin/service nessusd stop`
SuSE	`# /etc/rc.d/nessusd stop`
Debian	`# /etc/init.d/nessusd stop`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh stop`
Solaris	`# /etc/init.d/nessusd stop`
Ubuntu	`# /etc/init.d/nessusd stop`

Remoção do Nessus

A tabela a seguir apresenta instruções de remoção do servidor Nessus em todas as plataformas suportadas. Exceto pelas instruções usadas com o Mac OS X, as instruções fornecidas não excluirão os arquivos de configuração ou os arquivos que não faziam parte da instalação original. Os arquivos que faziam parte do pacote original, e que foram alterados desde a instalação, também não serão excluídos. Para excluir completamente os arquivos restantes, use o comando a seguir:

Linux e Solaris:

```
# rm -rf /opt/nessus
```

FreeBSD:

```
# rm -rf /usr/local/nessus/bin
```

Plataforma	Instruções de remoção
Red Hat ES 4 e CentOS 4 (32 bits); Red Hat ES 5, CentOS 5 e Oracle Linux 5 (32 e 64 bits); Red Hat ES 6, CentOS 6 e Oracle Linux 6 (32 e 64 bits)	

Comando de remoção	Para determinar o nome do pacote:
	`# rpm -qa | grep Nessus`
	Use o resultado do comando acima para remover o pacote:
	`# rpm -e <Package Name>`

Exemplo de resultado	`# rpm -qa | grep -i nessus`
	`Nessus-5.0.1-es5`
	`# rpm -e Nessus-5.0.1-es5`
	`#`

Fedora Core 16 (32 e 64 bits)	

Comando de remoção	Para determinar o nome do pacote:
	
	`# rpm -qa | grep Nessus`
	
	Use o resultado do comando acima para remover o pacote:
	
	`# rpm -e <Package Name>`

SuSE 10 (64 bits), 11 (32 e 64 bits)	

Comando de remoção	Para determinar o nome do pacote:
	
	`# rpm -qa | grep Nessus`
	
	Use o resultado do comando acima para remover o pacote:
	
	`# rpm -e <Package Name>`

Debian 6 (32 e 64 bits)	

Comando de remoção	Para determinar o nome do pacote:
	
	`# dpkg -l | grep -i nessus`
	
	Use o resultado do comando acima para remover o pacote:
	
	`# dpkg -r <package name>`

Exemplo de resultado	`# dpkg -l | grep nessus`
	`ii  nessus  5.0.1  Version 4 of the Nessus Scanner`
	
	`# dpkg -r nessus`
	`#`

Ubuntu 8.04, 9.10, 10.04 10.10 e 11.10 (32 e 64 bits)	

Comando de remoção	Para determinar o nome do pacote:
	
	`# dpkg -l | grep -i nessus`
	
	Use o resultado do comando acima para remover o pacote:
	
	`# dpkg -r <package name>`

Exemplo de resultado	`# dpkg -l | grep -i nessus`
	`ii  nessus  5.0.1  Version 4 of the Nessus Scanner`
	`#`

Solaris 10 (sparc)	
Comando de remoção	Parar o serviço **nessusd**: `# /etc/init.d/nessusd stop`

	Para determinar o nome do pacote:
	
	`# pkginfo | grep –i nessus`
	
	Parar remover o pacote do Nessus:
	
	`# pkgrm <package name>`

Exemplo de resultado	O exemplo a seguir descreve o resultado do comando anterior exibindo o pacote do Nessus:
	
	`# pkginfo | grep –i nessus`
	
	`application TNBLnessus The Nessus Network Vulnerability Scanner`
	`# pkgrm TNBLnessus`
	`#`

FreeBSD 9 (32 e 64 bits)	

Comando de remoção	Para parar o Nessus:
	
	`# killall nessusd`
	
	Para determinar o nome do pacote:
	
	`# pkg_info | grep -i nessus`
	
	Parar remover o pacote do Nessus:
	
	`# pkg_delete <package name>`

Exemplo de resultado	`# killall nessusd`
	
	`# pkg_info | grep -i nessus`
	`Nessus-5.0.1 A powerful security scanner`
	`# pkg_delete Nessus-5,0.1`
	`#`

Mac OS X	

Comando de remoção	Abra uma janela de terminal: Em “Applications” (Aplicativos), clique em “Utilities” (Utilitários) e, em seguida, clique em “Terminal” ou “X11”. Na janela de comando, use o comando “sudo” para executar um shell de raiz e exclua os diretórios do Nessus da seguinte maneira:
	
	`$ sudo /bin/sh`
	`Password:`
	`# ls -ld /Library/Nessus`
	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`# ls -ld /Applications/Nessus`
	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`

	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`# exit`

Exemplo de resultado	`$ sudo /bin/sh`
	`Password:`
	`# ls -ld /Library/Nessus`
	`drwxr-xr-x  6 root  admin  204 Apr  6 15:12 /Library/Nessus`
	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`ls: /Library/Nessus: No such file or directory`
	`# ls -ld /Applications/Nessus`
	`drwxr-xr-x  4 root  admin  136 Apr  6 15:12 /Applications/Nessus`
	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Client.pkg`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11 /Library/Receipts/Nessus Server.pkg`
	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`ls: /Library/Receipts/Nessus*: No such file or directory`
	`# exit`
	`$`

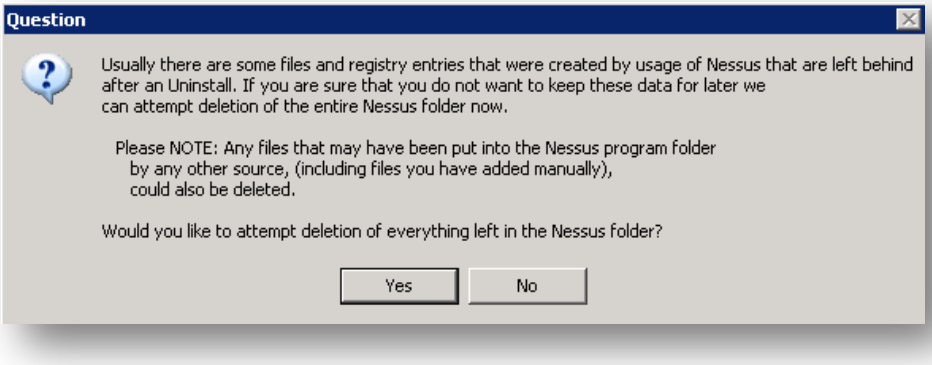
Observações	Não tente executar este processo se não estiver familiarizado com os comandos de shell do Unix. Os comandos “ls” estão incluídos para verificar se o nome do caminho foi digitado corretamente.

Windows

Atualizações

Atualização do Nessus 4.x

Ao atualizar o Nessus de uma versão 4.x para uma distribuição mais recente 5.x, o processo de atualização perguntará se o usuário deseja apagar todo o conteúdo do diretório Nessus. Selecione a opção “Yes” (Sim) para simular um processo de desinstalação. Se esta opção for selecionada, os usuários criados anteriormente, as políticas de varredura e os resultados das varreduras serão excluídos e o scanner deixará de ser registrado.


Question
Usually there are some files and registry entries that were created by usage of Nessus that are left behind after an Uninstall. If you are sure that you do not want to keep these data for later we can attempt deletion of the entire Nessus folder now.
Please NOTE: Any files that may have been put into the Nessus program folder by any other source, (including files you have added manually), could also be deleted.
Would you like to attempt deletion of everything left in the Nessus folder?
Yes
No

Clique em “Yes” (Sim) para permitir que o Nessus exclua toda a pasta do Nessus juntamente com todos os arquivos adicionados manualmente ou “No” (Não) para manter a pasta do Nessus junto com as varreduras, relatórios etc. existentes. Depois que a nova versão do Nessus for instalada, eles ainda estarão disponíveis para visualização e exportação.

Atualização do Nessus 3.x

A atualização direta do Nessus 3.0.x para Nessus 5.x não é compatível. No entanto, uma atualização para a versão 4 pode ser usada como uma etapa provisória para garantir que as configurações de varredura e políticas sejam preservadas. Se não for necessário preservar as configurações de varredura, primeiro desinstale o Nessus 3.x e, depois, instale uma nova cópia do Nessus 5.

Se “Yes” (Sím) for selecionado, **todos os arquivos do diretório Nessus serão excluídos**, incluindo os arquivos de log, os plugins personalizados adicionados manualmente e outros itens. Selecione esta opção com cuidado!

Instalação

Download do Nessus

Baixe a versão mais recente do Nessus em http://www.nessus.org/products/nessus/nessus-download-agreement ou por meio do Tenable Support Portal. O Nessus 5 está disponível para Windows XP, Server 2003, Server 2008, Vista e Windows 7. Verifique a integridade do pacote de instalação comparando o checksum MD5 do download com o checksum indicado no `MD5.asc` arquivo aqui.

O tamanho e nomes dos arquivos de distribuição do Nessus variam um pouco de uma versão para outra, mas têm cerca de 12 MB.

Instalação

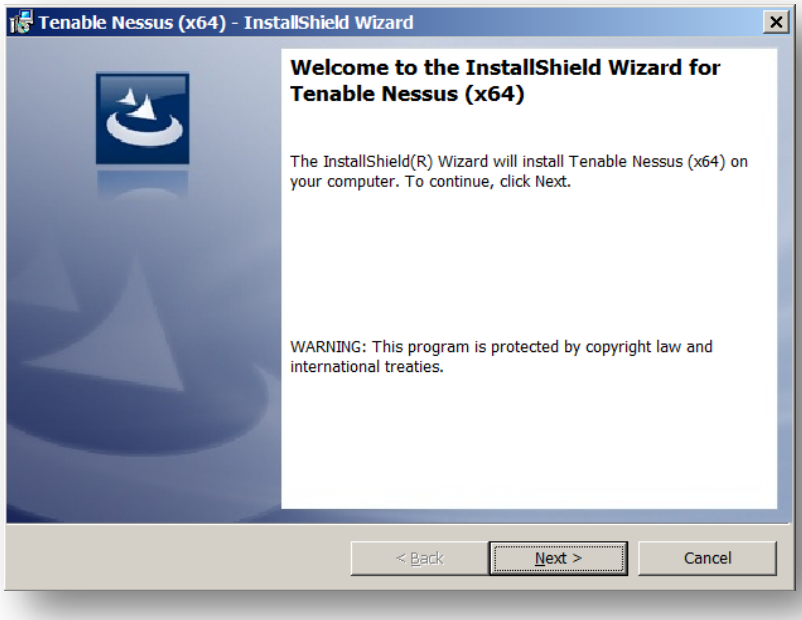
O Nessus é distribuído como um arquivo de instalação executável. Coloque o arquivo no sistema em que será instalado ou em uma unidade compartilhada que o sistema possa acessar.

É preciso instalar o Nessus com uma conta administrativa e não como um usuário sem privilégios. Se a mensagem de erro relacionada a permissões “Access Denied” (Acesso Negado) for exibida ou se ocorrerem erros que indiquem que uma ação ocorreu devido à falta de privilégios, verifique se está usando uma conta com privilégios administrativos. Se surgirem erros ao usar utilitários de linha de comando, execute `cmd.exe` privilégios de “Run as…” (Executar como...) configurados como “administrator” (administrador).

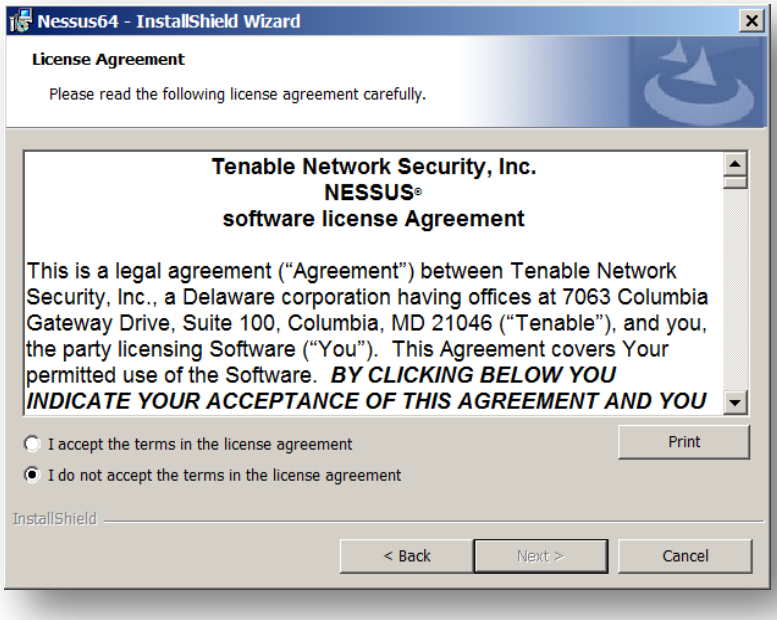
Alguns pacotes de software antivírus podem classificar o Nessus como um worm ou algum tipo de malware. Isto se deve ao grande número de conexões TCP geradas durante uma varredura. Se o software antivírus gerar um aviso, clique em “allow” (permitir) para que o Nessus possa continuar a varredura. A maioria dos pacotes AV também permite adicionar processos em uma lista de exceções. Adicione `Nessus.exe` e `Nessus-service.exe` à lista para prevenir esses avisos.

É recomendável obter um Activtion Code (Código de Ativação) de feed de plugin antes de iniciar o processo de instalação, uma vez que as informações serão necessárias para autenticar a GUI (interface do usuário) Nessus. Para obter mais informações sobre como obter um Activtion Code (Código de Ativação), leia a seção intitulada Inscrições em plugins de vulnerabilidades.

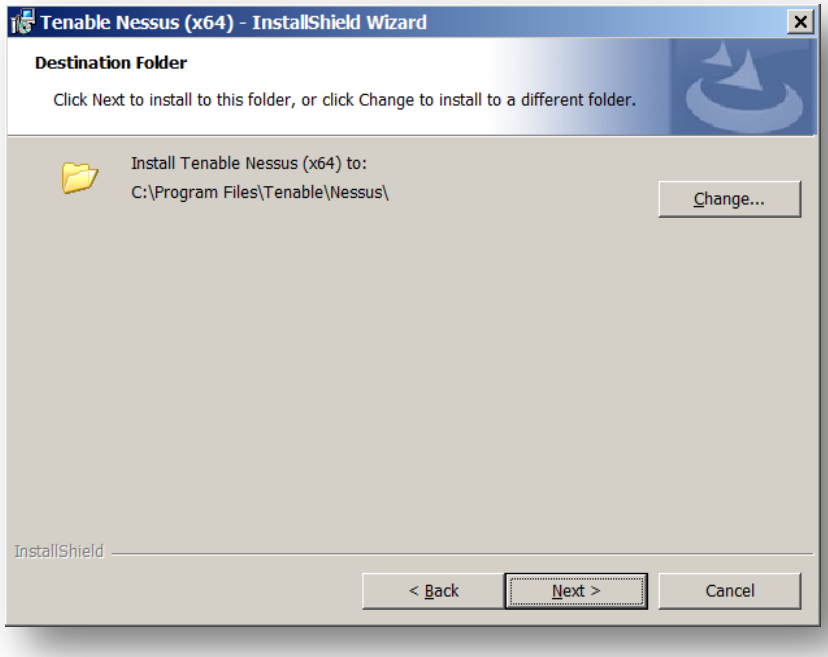
Problemas de instalação


Tenable Nessus (x64) - InstallShield Wizard
Welcome to the InstallShield Wizard for Tenable Nessus (x64)
The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

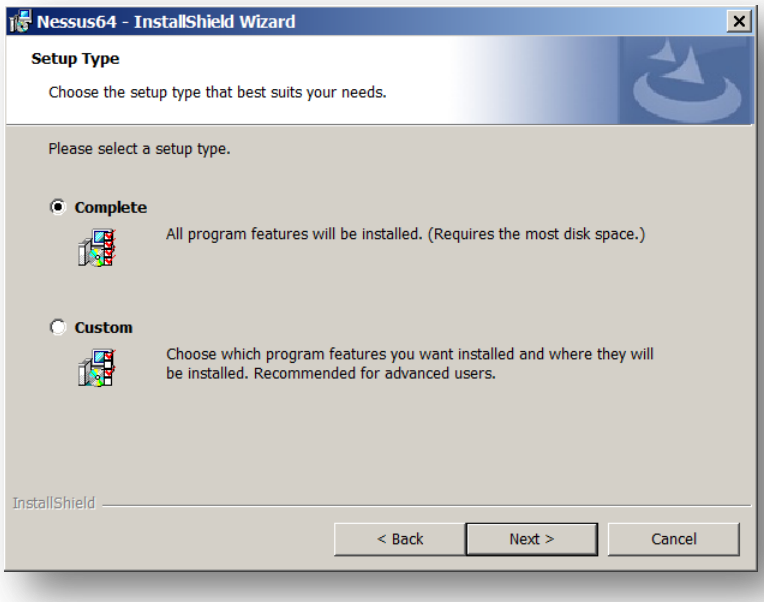
Durante o processo de instalação, o Nessus solicitará ao usuário algumas informações básicas. Antes de começar, o usuário deve aceitar o contrato de licença:


Nessus64 - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Tenable Network Security, Inc.
NESSUS®
software license Agreement
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

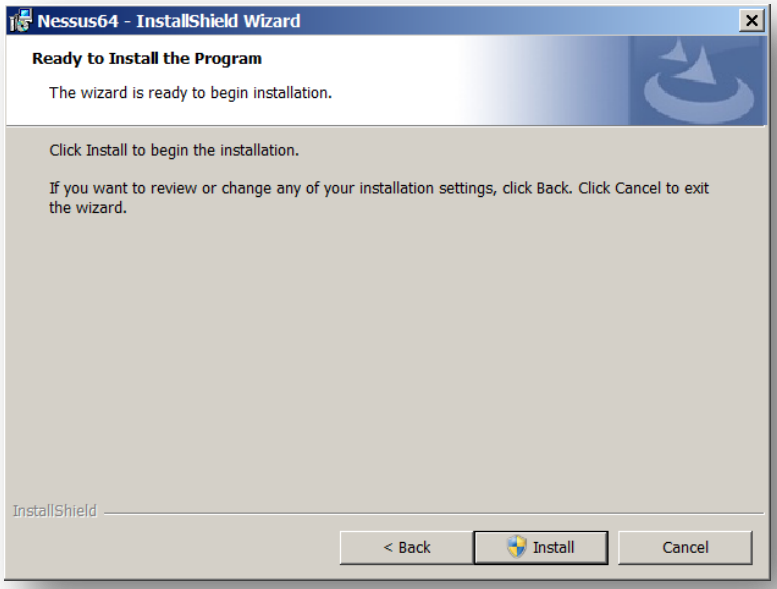
Depois de aceitar o contrato, escolha o local onde o Nessus será instalado:


Tenable Nessus (x64) - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Tenable Nessus (x64) to:
C:\Program Files\Tenable\Nessus\
Change...
InstallShield
< Back
Next >
Cancel

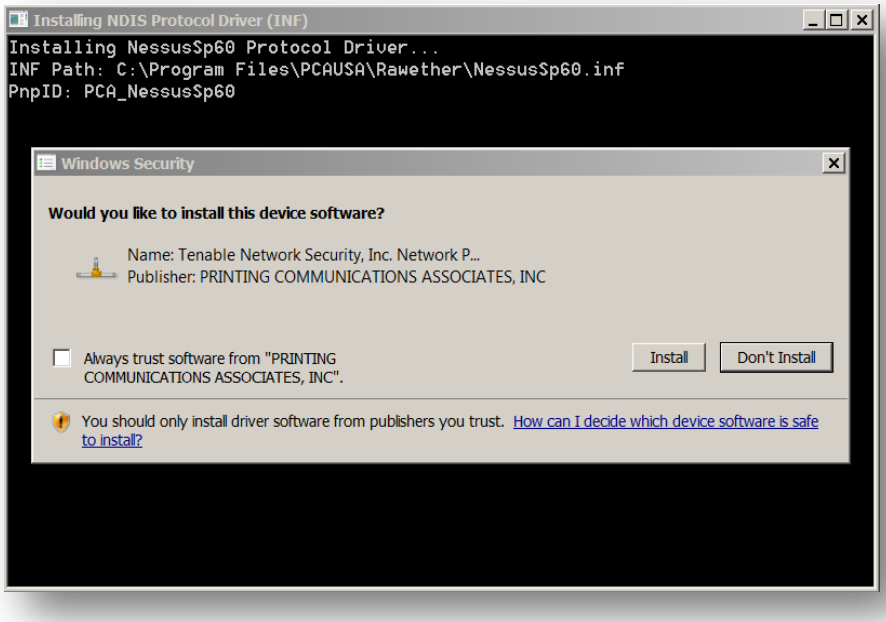
Quando solicitado para selecionar o “Setup Type” (Tipo de instalação), escolha “Complete” (Completo).


Nessus64 - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

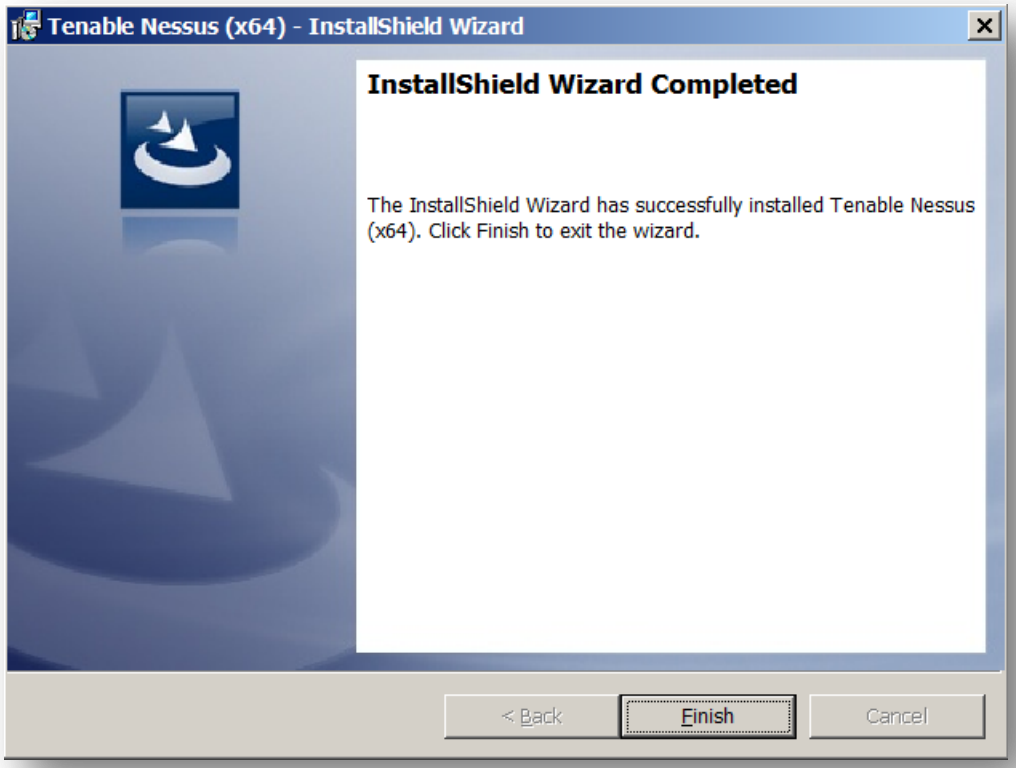
Será solicitado que você confirme a instalação:


Nessus64 - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

Após a instalação inicial ser concluída, o Nessus iniciará a instalação de um driver terceirizado usado para apoiar a comunicação entre o Ethernet e o Nessus:


Installing NDIS Protocol Driver (INF)
Installing NessusSp60 Protocol Driver...
INF Path: C:\Program Files\PCAUSA\Rawether\NessusSp60.inf
PnpID: PCA_NessusSp60
Windows Security
Would you like to install this device software?
Name: Tenable Network Security, Inc. Network P...
Publisher: PRINTING COMMUNICATIONS ASSOCIATES, INC
Always trust software from "PRINTING COMMUNICATIONS ASSOCIATES, INC".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Quando a instalação for concluída, clique em “Finish” (Concluir).

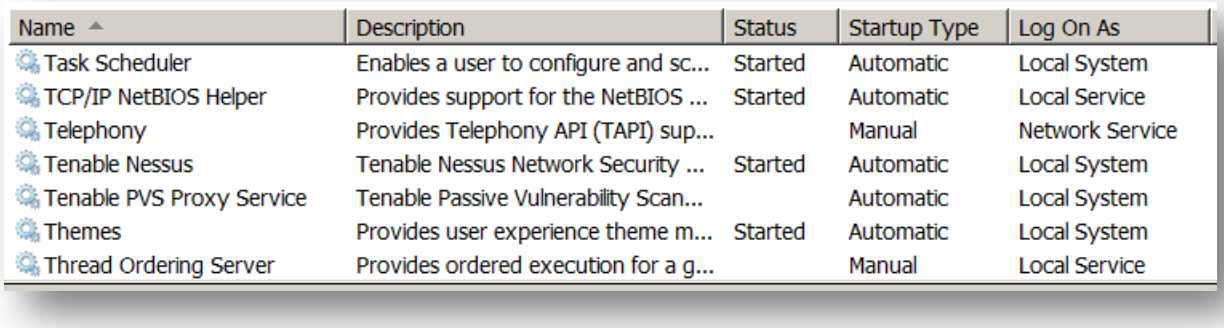

Tenable Nessus (x64) - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Tenable Nessus (x64). Click Finish to exit the wizard.
< Back
Finish
Cancel

Neste ponto, o Nessus prosseguirá carregando uma página no navegador padrão para controle da configuração inicial, que é discutido na seção "Registro de feed e configuração da GUI (interface do usuário)".

Iniciar e parar o Daemon Nessus

Durante a instalação e operação diária do Nessus, em geral não é necessário manipular o serviço do Nessus. Há ocasiões em que um administrador pode querer parar temporariamente ou reiniciar o serviço.

Isso pode ser feito em um sistema Windows abrindo o menu "Start" (Iniciar) e clicando em "Run" (Executar). Na caixa "Run" (Executar), digite "`services.msc`" para abrir o Windows Service Manager (Gerenciador de Serviços do Windows):



Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a user to configure and sc...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides support for the NetBIOS ...	Started	Automatic	Local Service
Telephony	Provides Telephony API (TAPI) sup...		Manual	Network Service
Tenable Nessus	Tenable Nessus Network Security ...	Started	Automatic	Local System
Tenable PVS Proxy Service	Tenable Passive Vulnerability Scan...		Automatic	Local System
Themes	Provides user experience theme m...	Started	Automatic	Local System
Thread Ordering Server	Provides ordered execution for a g...		Manual	Local Service

Clique com o botão direito no serviço "Tenable Nessus" para exibir uma caixa de diálogo que permite iniciar, parar, pausar, continuar ou reiniciar o serviço, dependendo do status atual.

Além disso, o serviço Nessus pode ser manipulado na linha de comandos. Para obter mais informações, consulte a seção "Manipulação do serviço Nessus por meio de CLI do Windows" neste documento.

Remoção do Nessus

Para remover o Nessus, abra o Painel de Controle e selecione "**Add or Remove Programs**" (Adicionar ou remover programas). Selecione "**Tenable Nessus**" (Tenable Nessus) e clique no botão "**Change/Remove**" (Desinstalar/Alterar). Isto abrirá o assistente de instalação/desinstalação. Siga as instruções do assistente para excluir completamente o Nessus. O usuário poderá optar por remover inteiramente a pasta do Nessus. Responda "Yes" (Sí) somente se não desejar manter nenhum resultado de varreduras ou políticas gerado.

Ao desinstalar o Nessus, o Windows perguntará se deseja continuar, mas mostrará um arquivo **`.msi`** aparentemente desconhecido. Por exemplo:

C:\Windows\Installer\778608.msi
Publisher: Unknown

Isto ocorre devido ao Windows manter uma cópia interna do programa de instalação do Nessus e usá-lo para iniciar o processo de desinstalação. A solicitação pode ser aceita com segurança.

Mac OS X

Atualizações

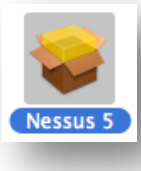
A atualização de uma versão antiga do Nessus é semelhante a uma nova instalação. Baixe o arquivo **`Nessus-5.x.x.dmg.gz`** e, em seguida, clique duas vezes sobre ele para descompactá-lo. Clique duas vezes no arquivo **`Nessus-5.x.x.dmg`** para montar a imagem de disco e fazer com que apareça em "Devices" (Dispositivos) no "Finder" (Localizador). Quando o volume "Nessus 5" aparecer no "Finder" (Localizador), clique duas vezes no arquivo Nessus 5. Quando a instalação for concluída, faça o login no Nessus por meio do navegador em https://localhost:8834.

Instalação

Baixe a versão mais recente do Nessus em http://www.nessus.org/products/nessus/nessus-download-agreement ou por meio do Tenable Support Portal. O Nessus está disponível para o Mac OS X 10.6 e 10.7. Verifique a integridade do pacote de instalação ao comparar o checksum MD5 do download com o checksum MD5 listado no arquivo **`MD5.asc`** aqui.

O tamanho e nomes dos arquivos de distribuição do Nessus para Mac OS X variam um pouco de uma versão para outra, mas têm cerca de 45 MB.

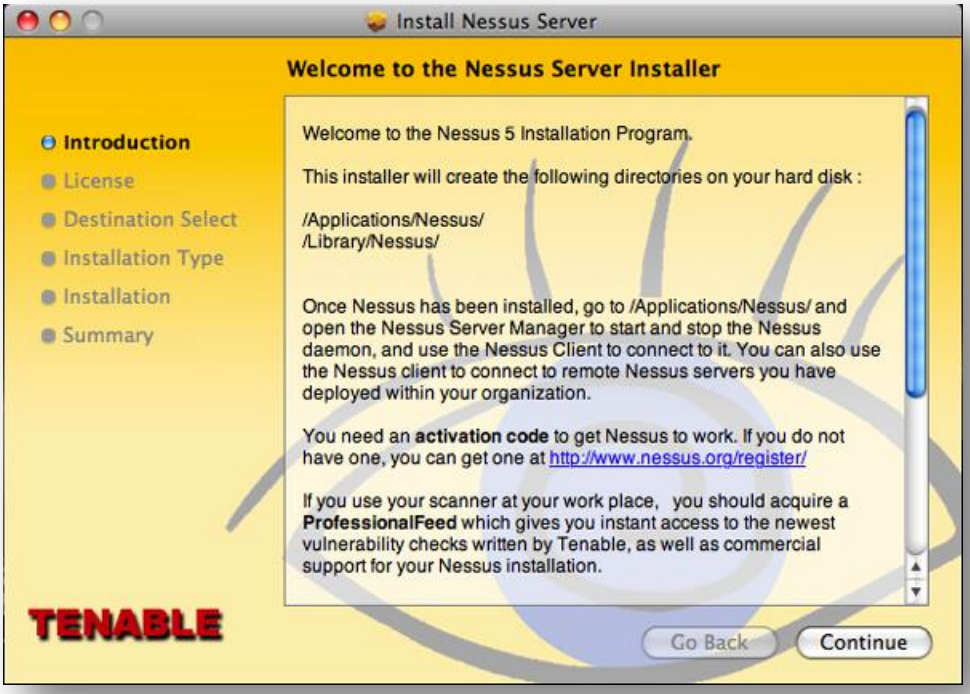
Para instalar o Nessus no Mac OS X, baixe o arquivo **`Nessus-5.x.x.dmg.gz`** e clique duas vezes nele para descompactá-lo. Clique duas vezes no arquivo **`Nessus-5.x.x.dmg`** para montar a imagem de disco e fazer com que apareça em "Devices" (Dispositivos) no "Finder" (Localizador). Quando o volume "`Nessus 5`" aparecer no "Finder" (Localizador), clique duas vezes no arquivo **`Nessus 5`** conforme exemplo a seguir:



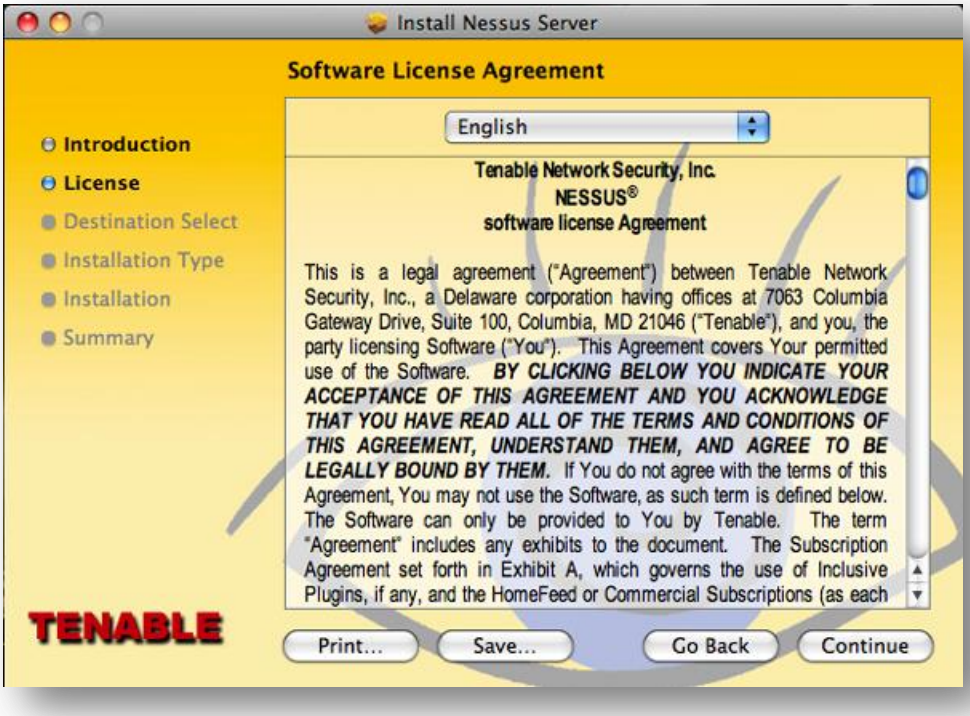
Observe que será preciso digitar o nome de usuário e a senha de administrador uma vez durante a instalação.

Problemas de instalação

A instalação será exibida da seguinte maneira:

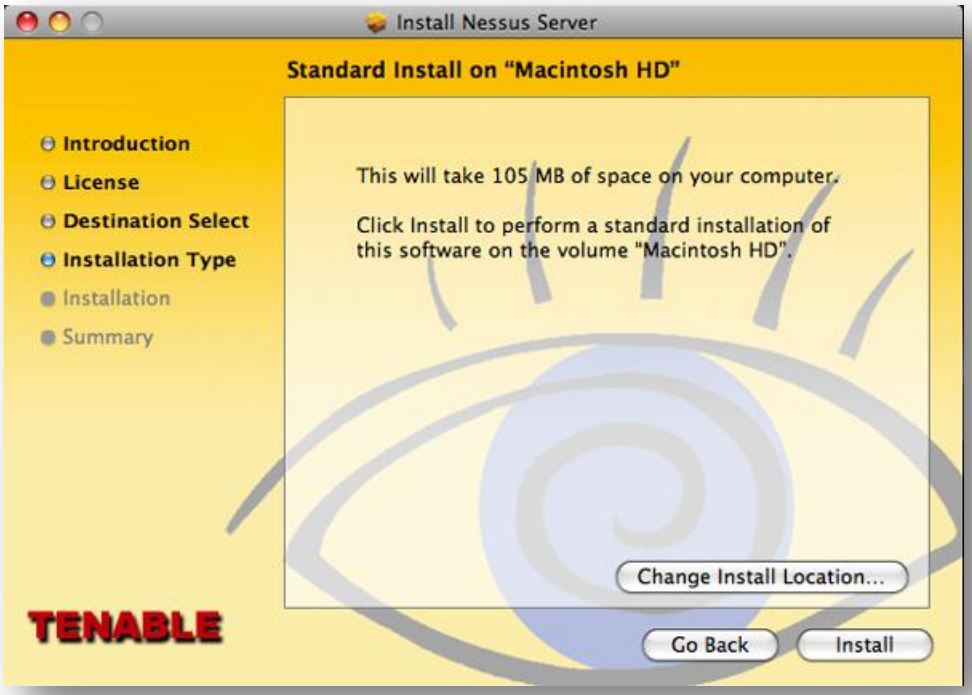

Install Nessus Server
Welcome to the Nessus Server Installer
Introduction
License
Destination Select
Installation Type
Installation
Summary
Welcome to the Nessus 5 Installation Program.
This installer will create the following directories on your hard disk :
/Applications/Nessus/
/Library/Nessus/
Once Nessus has been installed, go to /Applications/Nessus/ and open the Nessus Server Manager to start and stop the Nessus daemon, and use the Nessus Client to connect to it. You can also use the Nessus client to connect to remote Nessus servers you have deployed within your organization.
You need an activation code to get Nessus to work. If you do not have one, you can get one at http://www.nessus.org/register/
If you use your scanner at your work place, you should acquire a ProfessionalFeed which gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.
TENABLE
Go Back
Continue

Clique em “Continue” (Continuar) para exibir a licença do software. Clique em “Continue” (Continuar) novamente. Uma caixa de diálogo será exibida solicitando que você aceite os termos da licença antes de continuar:


Install Nessus Server
Software License Agreement
Introduction
License
Destination Select
Installation Type
Installation
Summary
English
Tenable Network Security, Inc.
NESSUS®
software license Agreement
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the HomeFeed or Commercial Subscriptions (as each
TENABLE
Print...
Save...
Go Back
Continue

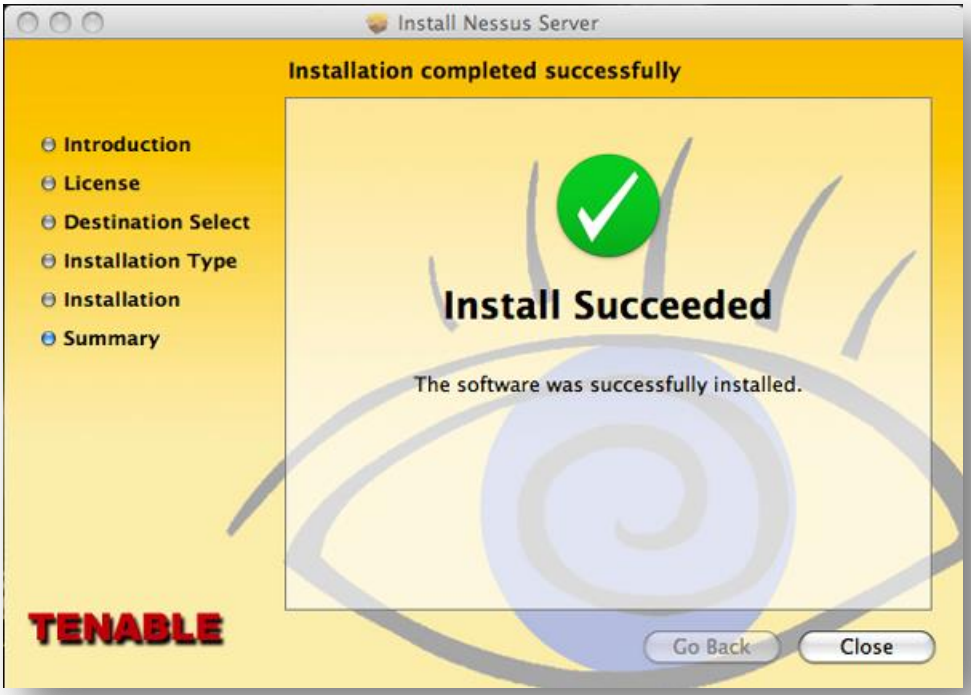
Install Nessus Server
To continue installing the software you must agree to the terms of the software license agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.
Read License
Disagree
Agree
Summary
party licensing Software ("You"). This Agreement covers Your permitted

Depois de aceitar a licença, outra caixa de diálogo será exibida, que permite alterar o local de instalação padrão, conforme indicado a seguir:



Clique no botão “Install” (Instalar) para continuar a instalação. Neste momento, o usuário deverá digitar o nome de usuário e a senha de administrador:

Quando a seguinte tela for exibida a instalação terá sido concluída com êxito:



Neste ponto, o Nessus prosseguirá carregando uma página no navegador padrão para controle da configuração inicial, que é discutido na seção "Registro de feed e configuração da GUI (interface do usuário)".

Iniciar e parar o serviço Nessus

Após a instalação, o serviço **nessusd** será iniciado. Durante cada reinicialização, o serviço será iniciado automaticamente. Se houver um motivo para iniciar ou parar o serviço, isto pode ser feito por meio da janela Terminal (linha de comando). O comando deve ser executado como "root" ou por meio de **sudo**:

Ação	Comando de gerenciamento do nessusd
Iniciar	`# launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`
Parar	`# launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`

Remoção do Nessus

Para remover o Nessus, exclua os seguintes diretórios:

```
/Library/Nessus
/Applications/Nessus
/Library/Receipts/Nessus*
```

Se não estiver familiarizado com o uso das linhas de comando do Unix em um sistema Mac OS X, entre em contato com o serviço de assistência da Tenable Support.

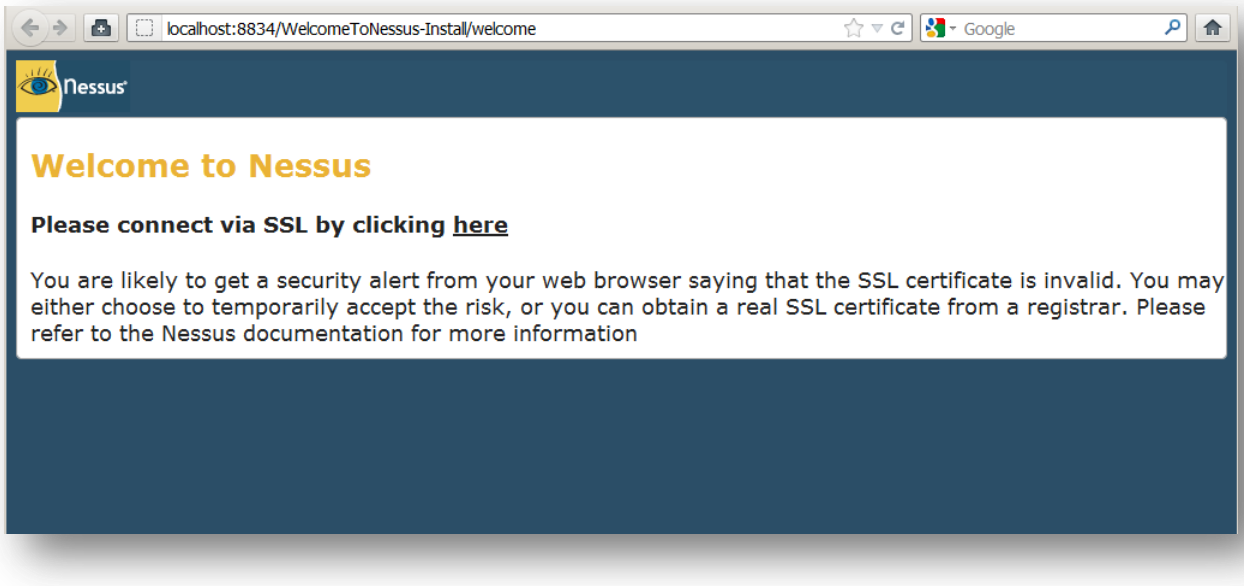
Existem ferramentas grátis, como o “DesInstaller.app” (http://www.macupdate.com/info.php/id/7511) e o “CleanApp” (http://www.macupdate.com/info.php/id/21453/cleanapp), que também podem ser usadas para remover o Nessus. A Tenable não garante o uso dessas ferramentas, que não foram avaliadas especificamente para a remoção do Nessus.

Registro de feed e configuração da GUI (interface do usuário)

Esta seção descreve como configurar o servidor Nessus 5 em todas as plataformas. A partir do Nessus 5, as opções de configuração iniciais, tais como opções de proxy e fornecimento de um Activtion Code (Código de Ativação), são realizadas por meio de um processo baseado na Web. Após a instalação do Nessus, o usuário terá seis horas para completar o processo de registro por razões de segurança. Se o registro não for completado nesse período, reinicie o **`nessusd`** e o processo de registro.

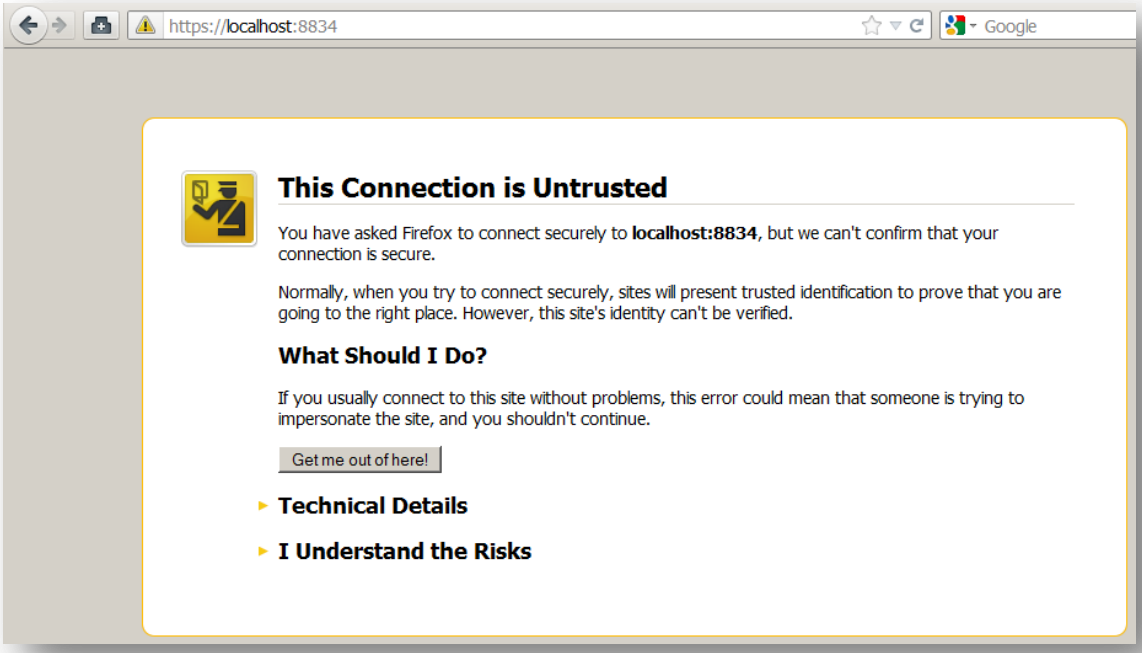
O Nessus Server Manager usado no Nessus 4 foi descontinuado.

Se o software de instalação não abrir o navegador com a página de configuração, abra o navegador e vá para a página **Erro! A referência de hyperlink não é válida.** (ou URL fornecido durante o processo de instalação) para iniciar o processo. Nota: As instalações em ambiente Unix podem gerar um URL com um nome de host correspondente que não está no DNS (por exemplo: http://mybox:8834/). Se o nome não estiver no DNS, será preciso se conectar ao servidor Nessus com um endereço IP ou nome DNS válido.

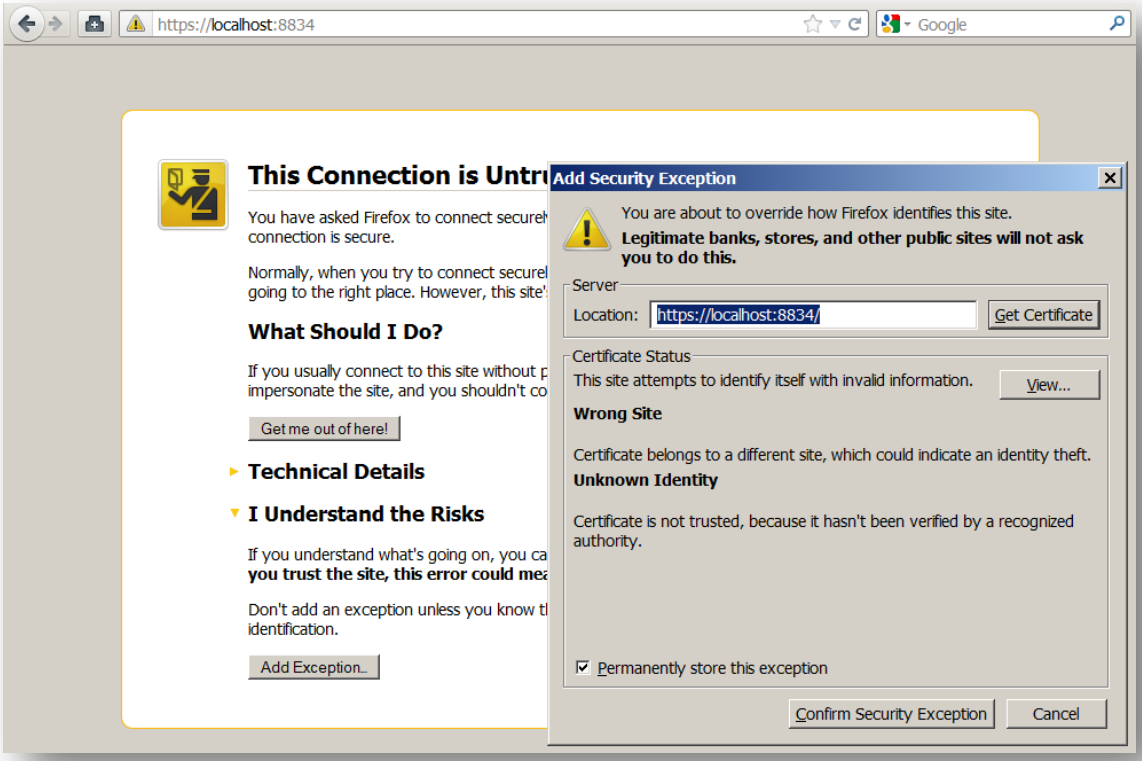

localhost:8834/WelcomeToNessus-Install/welcome
Google
Nessus
Welcome to Nessus
Please connect via SSL by clicking here
You are likely to get a security alert from your web browser saying that the SSL certificate is invalid. You may either choose to temporarily accept the risk, or you can obtain a real SSL certificate from a registrar. Please refer to the Nessus documentation for more information

A tela inicial serve como um aviso de que todo o tráfego da GUI (interface do usuário) Nessus é protegido por SSL (HTTPS). Ao tentar se conectar ao servidor da Web do Nessus pela primeira vez, o navegador exibirá algum tipo de erro indicando que o site não é confiável, devido ao certificado SSL autoassinado: Para a primeira conexão, aceite o certificado para prosseguir com a configuração. As instruções para instalação de um certificado personalizado são descritas neste documento, na seção “Configuração do Nessus com certificado SSL personalizado”.

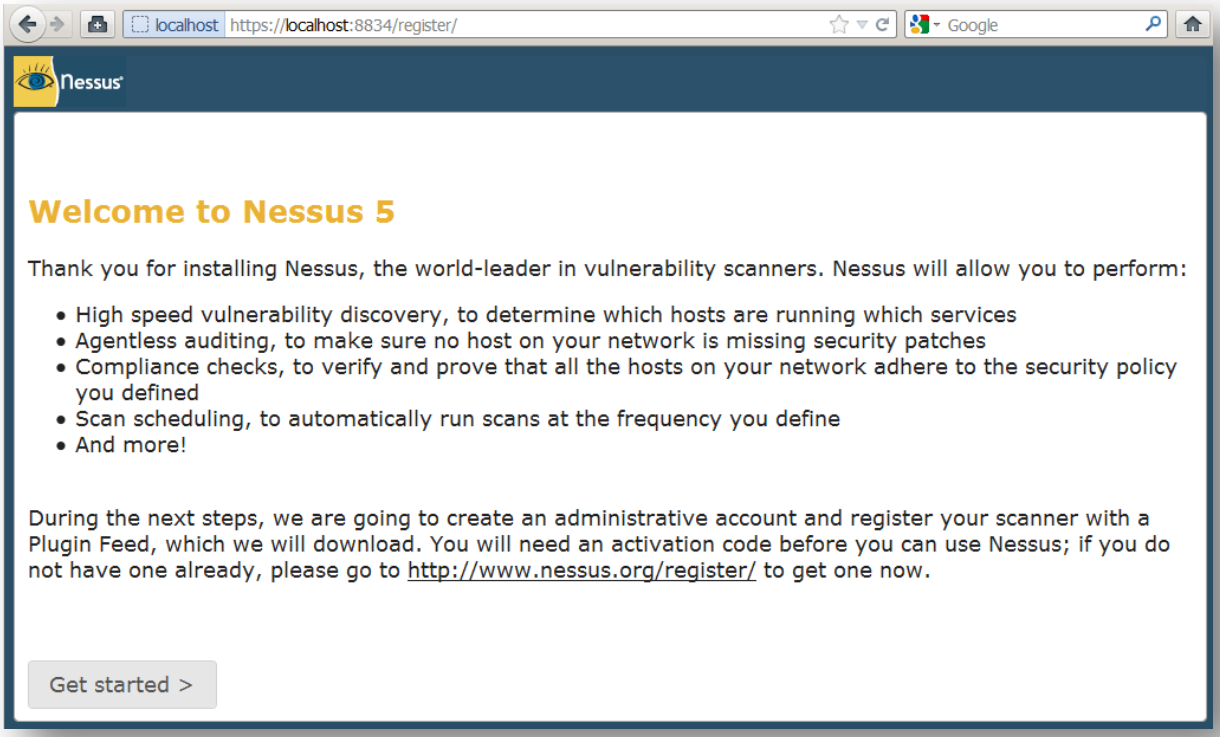
Devido à implementação técnica de certificados SSL, não é possível enviar um certificado com o Nessus que seja confiável para os navegadores. Para evitar este aviso, deve-se usar um certificado personalizado para a sua organização.


https://localhost:8834
Google
This Connection is Untrusted
You have asked Firefox to connect securely to localhost:8834, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

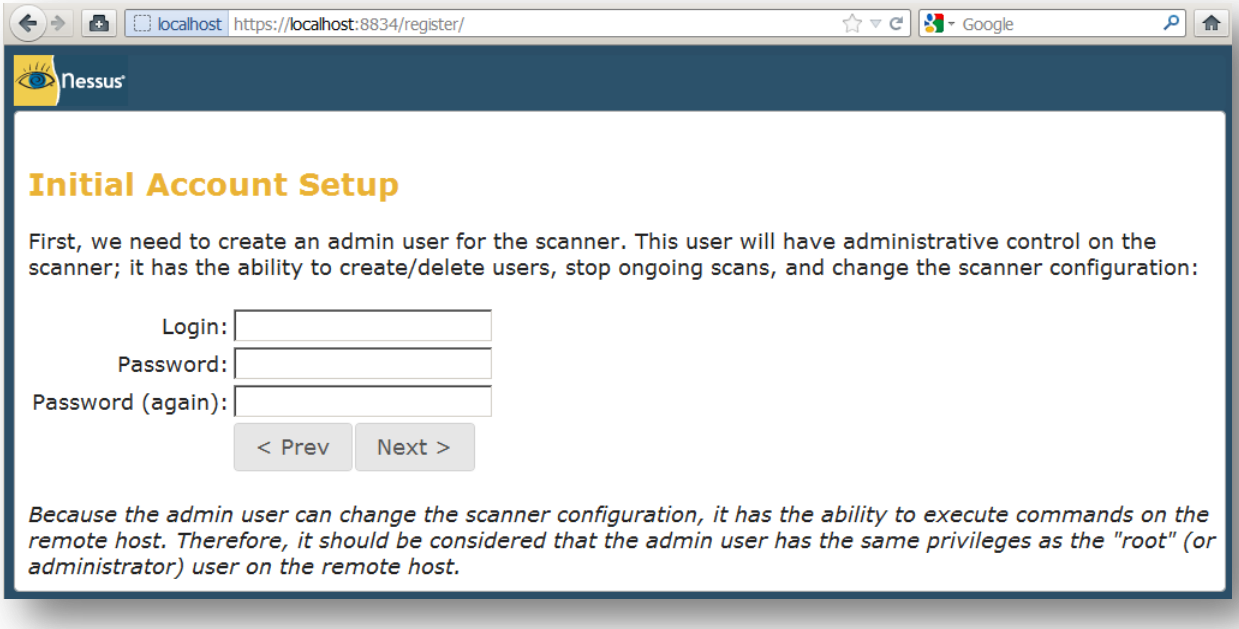
Dependendo do navegador usado, pode haver um diálogo adicional que fornece a capacidade de aceitar o certificado:


https://localhost:8834
Google
This Connection is Untr
You have asked Firefox to connect securel
connection is secure.
Normally, when you try to connect securel
going to the right place. However, this site'
What Should I Do?
If you usually connect to this site without p
impersonate the site, and you shouldn't co
Get me out of here!
Technical Details
I Understand the Risks
If you understand what's going on, you ca
you trust the site, this error could mea
Don't add an exception unless you know t
identification.
Add Exception...
Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://localhost:8834/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

Uma vez aceito, o usuário será redirecionado para a tela de registro inicial que inicia a navegação:

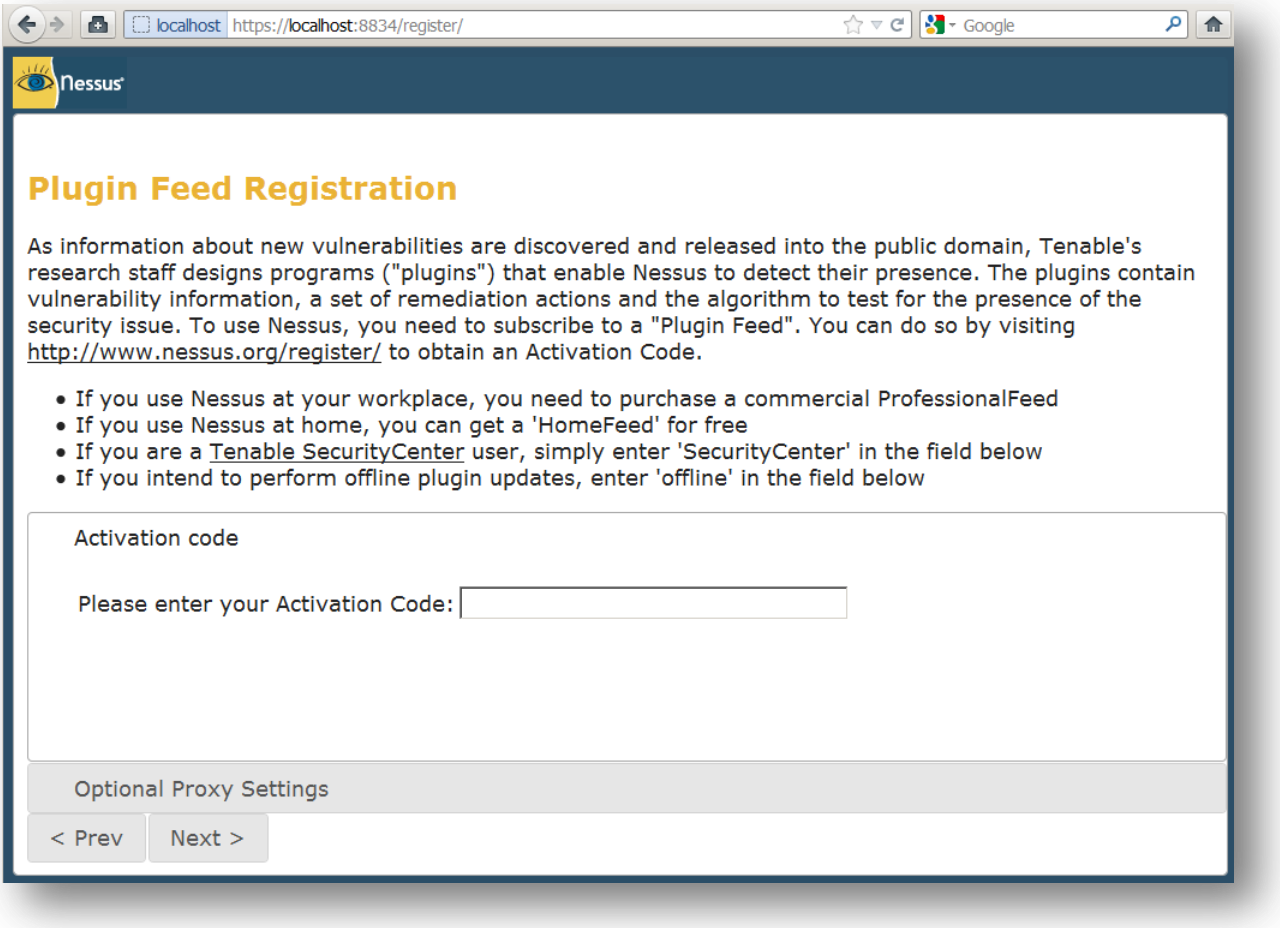

localhost https://localhost:8834/register/
Google
Nessus
Welcome to Nessus 5
Thank you for installing Nessus, the world-leader in vulnerability scanners. Nessus will allow you to perform:
• High speed vulnerability discovery, to determine which hosts are running which services
• Agentless auditing, to make sure no host on your network is missing security patches
• Compliance checks, to verify and prove that all the hosts on your network adhere to the security policy you defined
• Scan scheduling, to automatically run scans at the frequency you define
• And more!
During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download. You will need an activation code before you can use Nessus; if you do not have one already, please go to http://www.nessus.org/register/ to get one now.
Get started >

O primeiro passo é criar uma conta para o servidor Nessus. A conta inicial será um administrador, que terá acesso à execução de comandos no sistema operacional instalado no Nessus, por isso, deve ser considerada da mesma maneira que qualquer outra conta de administrador:


localhost https://localhost:8834/register/
Google
Nessus
Initial Account Setup
First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; it has the ability to create/delete users, stop ongoing scans, and change the scanner configuration:
Login:
Password:
Password (again):
< Prev
Next >
Because the admin user can change the scanner configuration, it has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.

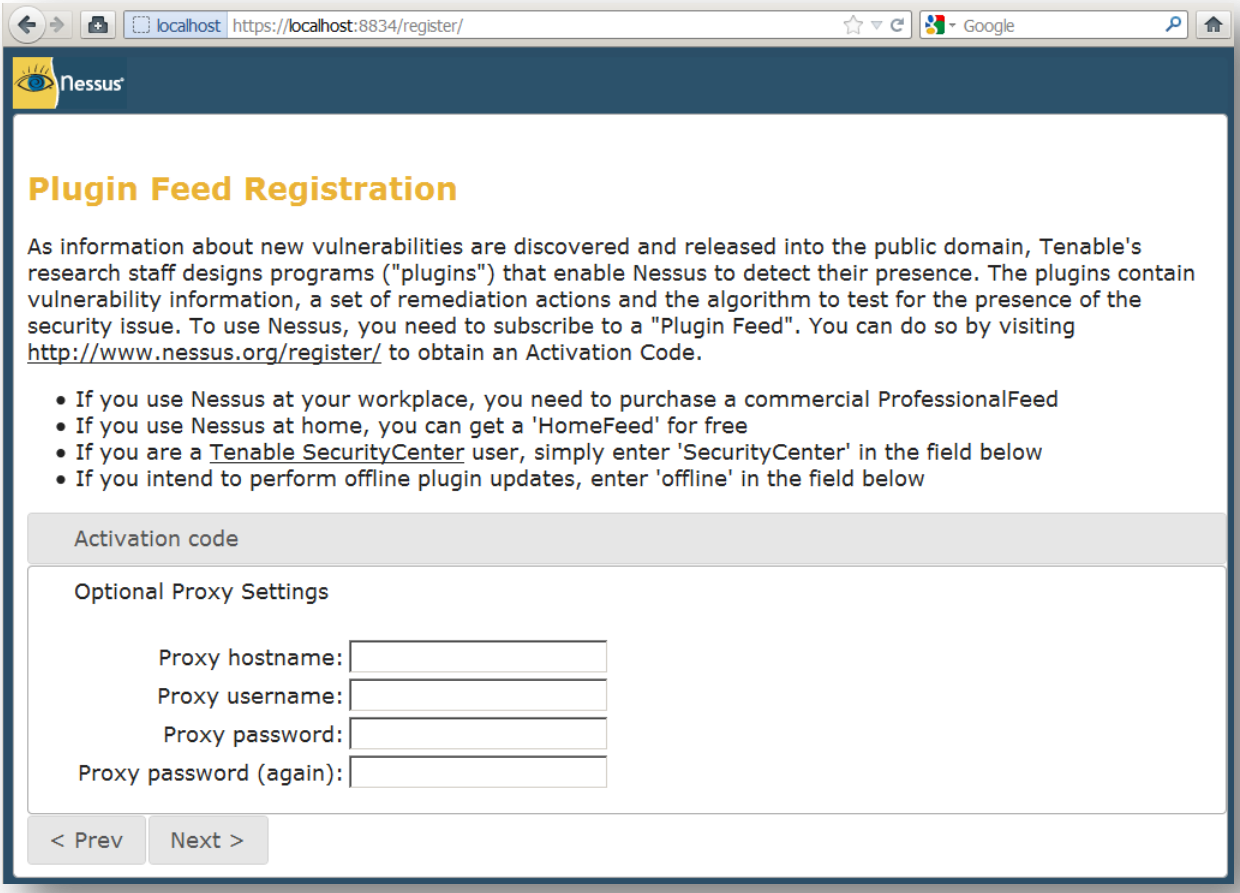
A tela seguinte solicita um Activtion Code (Código de Ativação) do plugin e permite definir as configurações de proxy opcionais.

Se o Tenable SecurityCenter for usado, o Código de Ativação e as atualizações do plugin serão gerenciadas por meio do SecurityCenter. Para se comunicar com o SecurityCenter, o Nessus precisa ser iniciado e, para isso, requer um Activtion Code (Código de Ativação) válido e plugins. Para fazer com que o Nessus ignore essa exigência e seja iniciado (para poder receber as informações do SecurityCenter), digite “SecurityCenter” (diferencia maiúsculas de minúsculas) sem aspas na caixa Activation Code (Código de ativação). Inicie o serviço nessusd para concluir a instalação e configuração iniciais do scanner Nessus e prossiga à seção “Como trabalhar como SecurityCenter”.

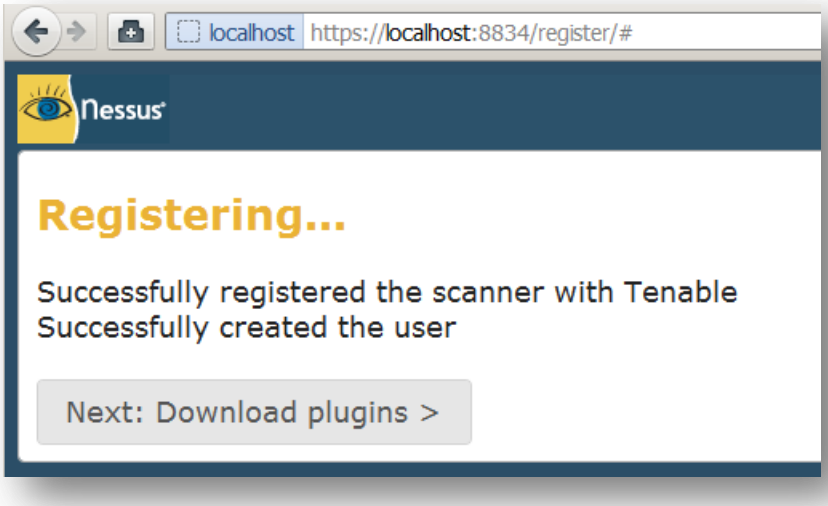

localhost
https://localhost:8834/register/
Google
Nessus
Plugin Feed Registration
As information about new vulnerabilities are discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, a set of remediation actions and the algorithm to test for the presence of the security issue. To use Nessus, you need to subscribe to a "Plugin Feed". You can do so by visiting http://www.nessus.org/register/ to obtain an Activation Code.
If you use Nessus at your workplace, you need to purchase a commercial ProfessionalFeed
If you use Nessus at home, you can get a 'HomeFeed' for free
If you are a Tenable SecurityCenter user, simply enter 'SecurityCenter' in the field below
If you intend to perform offline plugin updates, enter 'offline' in the field below
Activation code
Please enter your Activation Code:
Optional Proxy Settings
< Prev
Next >

Se a cópia do Nessus não for registrada, o usuário não receberá plugins atualizados e não poderá iniciar o servidor Nessus. Nota: O Activtion Code (Código de Ativação) **não** diferencia maiúsculas de minúsculas.

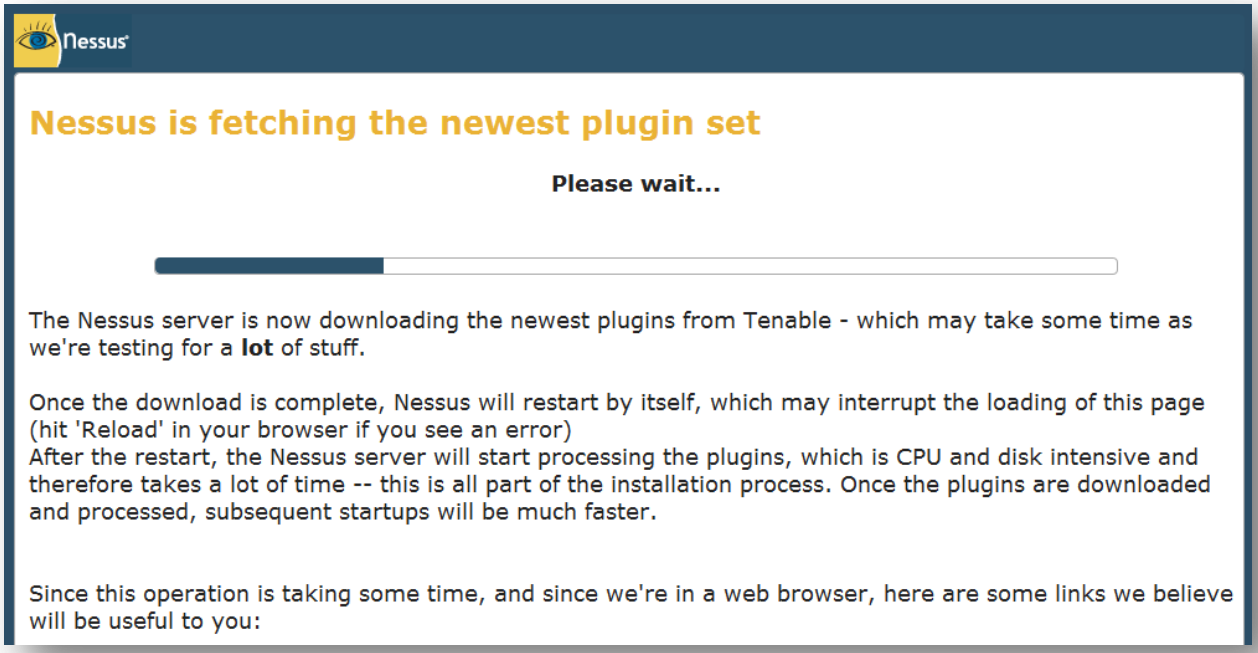
Se o servidor Nessus estiver em uma rede que usa um proxy para se comunicar com a Internet, clique em “**Optional Proxy Settings**” (Configurações de proxy opcionais) para inserir as informações correspondentes. As configurações de proxy podem ser adicionadas a qualquer momento após o término da instalação.


localhost https://localhost:8834/register/
Google
Nessus
Plugin Feed Registration
As information about new vulnerabilities are discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, a set of remediation actions and the algorithm to test for the presence of the security issue. To use Nessus, you need to subscribe to a "Plugin Feed". You can do so by visiting http://www.nessus.org/register/ to obtain an Activation Code.
If you use Nessus at your workplace, you need to purchase a commercial ProfessionalFeed
If you use Nessus at home, you can get a 'HomeFeed' for free
If you are a Tenable SecurityCenter user, simply enter 'SecurityCenter' in the field below
If you intend to perform offline plugin updates, enter 'offline' in the field below
Activation code
Optional Proxy Settings
Proxy hostname:
Proxy username:
Proxy password:
Proxy password (again):
< Prev
Next >

Após concluir a configuração do Activtion Code (Código de Ativação) e das definições de proxy **opcionais**, clique em "**Next**" (Avançar) para registrar o scanner:

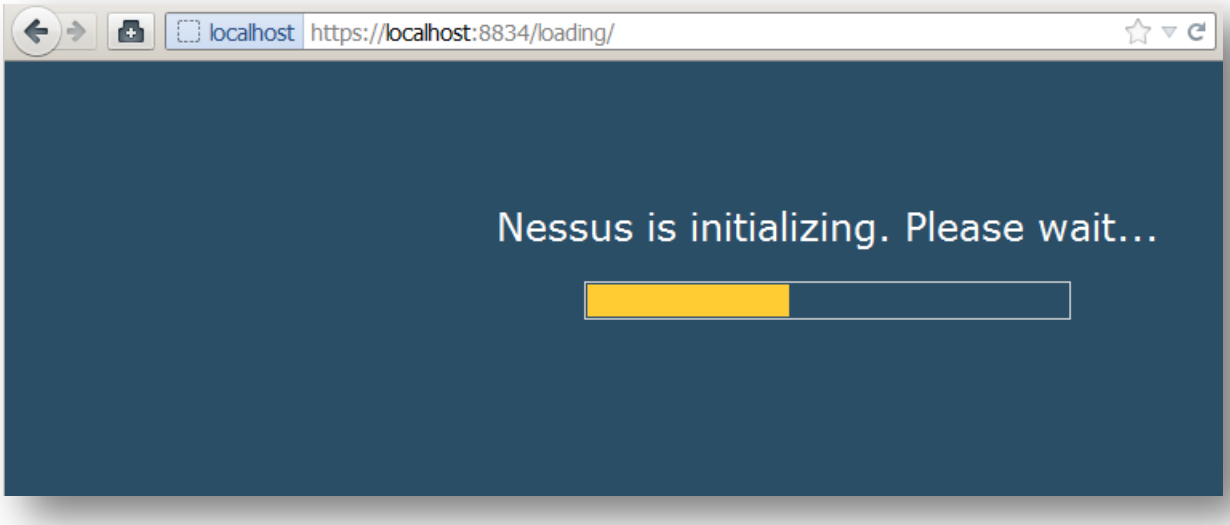


Após o registro, o Nessus deve baixar os plugins da Tenable. Este processo pode demorar vários minutos, pois transfere uma quantidade considerável de dados para a máquina, verifica a integridade do arquivo e agrupa-os em um banco de dados interno:

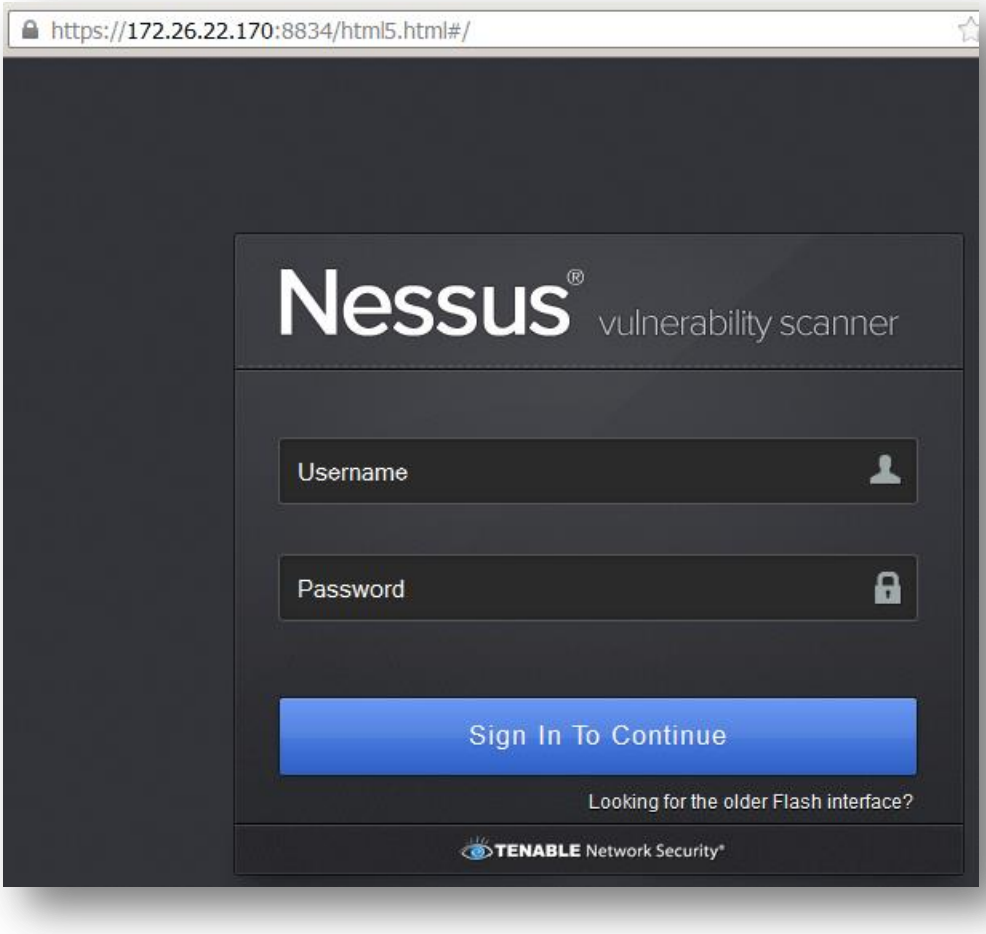

Nessus
Nessus is fetching the newest plugin set
Please wait...
The Nessus server is now downloading the newest plugins from Tenable - which may take some time as we're testing for a lot of stuff.
Once the download is complete, Nessus will restart by itself, which may interrupt the loading of this page (hit 'Reload' in your browser if you see an error)
After the restart, the Nessus server will start processing the plugins, which is CPU and disk intensive and therefore takes a lot of time -- this is all part of the installation process. Once the plugins are downloaded and processed, subsequent startups will be much faster.
Since this operation is taking some time, and since we're in a web browser, here are some links we believe will be useful to you:

Depois do registro inicial, o Nessus baixará e reunirá os plugins obtidos da porta 443 de plugins.nessus.org, plugins-customers.nessus.org **ou** plugins-us.nessus.org em segundo plano.

Uma vez que os plugins sejam baixados e compilados, a GUI (interface do usuário) Nessus será iniciada juntamente com o servidor Nessus:



Após a inicialização, o Nessus está pronto para uso!



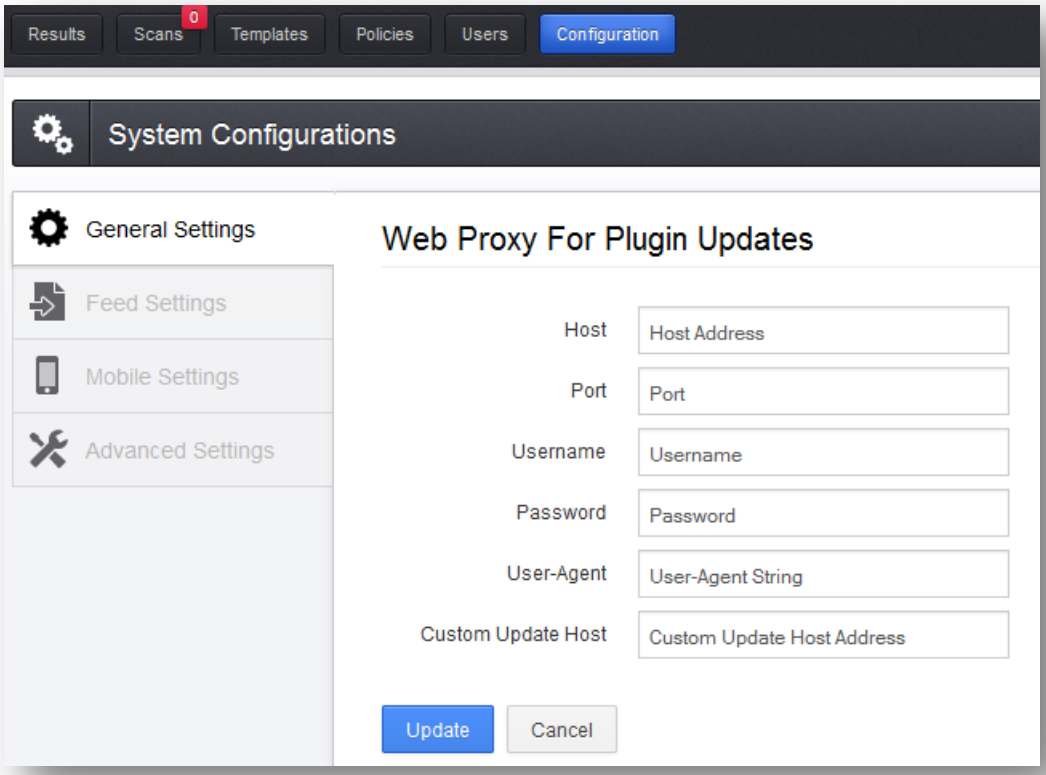
Usando as credenciais administrativas criadas durante a instalação, faça login na interface do Nessus para verificar o acesso.

Configuração

Com o lançamento do Nessus 5, toda a configuração do servidor Nessus é gerenciada por meio da GUI (Interface do usuário)). O arquivo **`nessusd.conf`** foi descontinuado. As configurações de proxy, o registro de inscrição de feed e as atualizações offline também são gerenciados por meio da GUI (interface do usuário).

Configurações de proxy da Web

No cabeçalho "**Configuration**" (Configuração), a guia "**Settings**" (Definições) permite configurar um proxy da Web para atualizações de plugins. Isto é necessário se a sua organização exigir que todo o tráfego da Web seja direcionado por meio de um proxy corporativo:



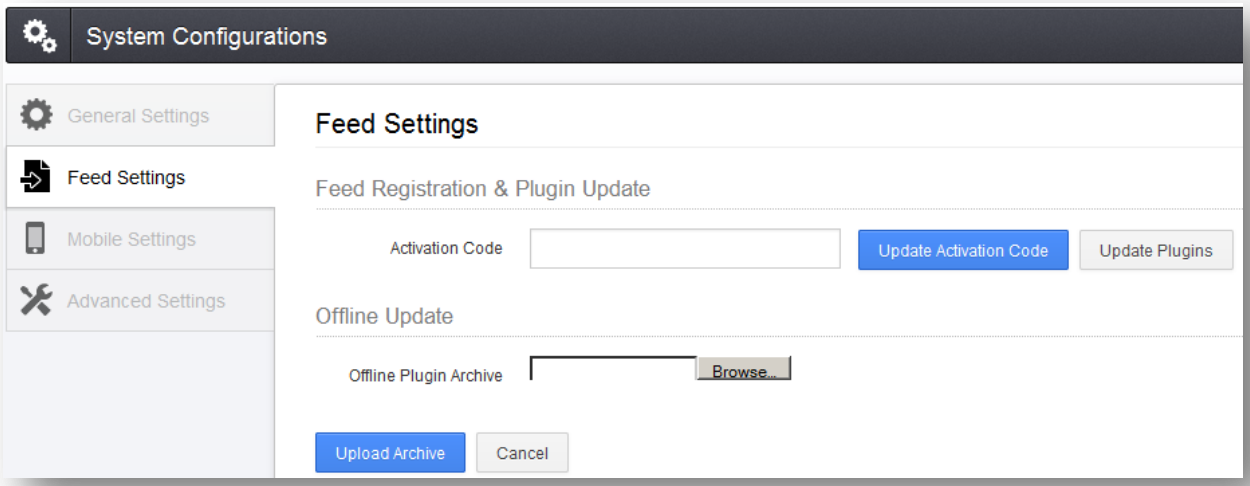
Há seis campos que controlam as configurações de proxy, mas apenas o host e a porta são obrigatórios. Opcionalmente, um nome de usuário e senha podem ser fornecidos, se necessário.

Opção	Descrição
Host	O host ou IP do proxy (por exemplo: proxy.example.com).
Port (Porta)	A porta do proxy (por exemplo: 8080).
Username	Opcional: Usado se o nome de usuário for necessário para uso do proxy (por exemplo: “jdoe”).
Password	Opcional: Usado se a senha for necessária para uso do proxy (por exemplo: “guineapigs”).
User-Agent	Opcional: Se o proxy em uso filtrar agentes de usuário HTTP específicos, uma string user-agent personalizada pode ser fornecida.
Custom Update Host	Opcional: Esta opção pode ser usada para forçar o Nessus a atualizar plugins de um host específico. Por exemplo: se os plugins forem atualizados de um site residente nos Estados Unidos, pode-se especificar “plugins-us.nessus.org”.

A partir do Nessus 4.2, os scanners do Microsoft Windows permitem a autenticação por proxy, inclusive NTLM.

Redefinir códigos de ativação e atualizações off-line

Depois de o Activation Code (Código de Ativação) inicial ser inserido durante o processo de configuração, as alterações subsequentes do Código de ativação serão feitas por meio da guia “**Feed Settings**” (Configurações de feed). Insira o novo código no campo “Activation Code” e clique em “Save” para atualizar o scanner Nessus com o novo código (por exemplo, ao atualizar um HomeFeed para ProfessionalFeed).



Você também pode forçar a atualização dos plugins em qualquer ocasião, ao clicar no botão “Update Plugins” (Atualizar plugins). Se uma atualização de plugin falhar por qualquer motivo (por exemplo, interrupção da conectividade de rede), o Nessus tentará novamente no intervalo de dez minutos.

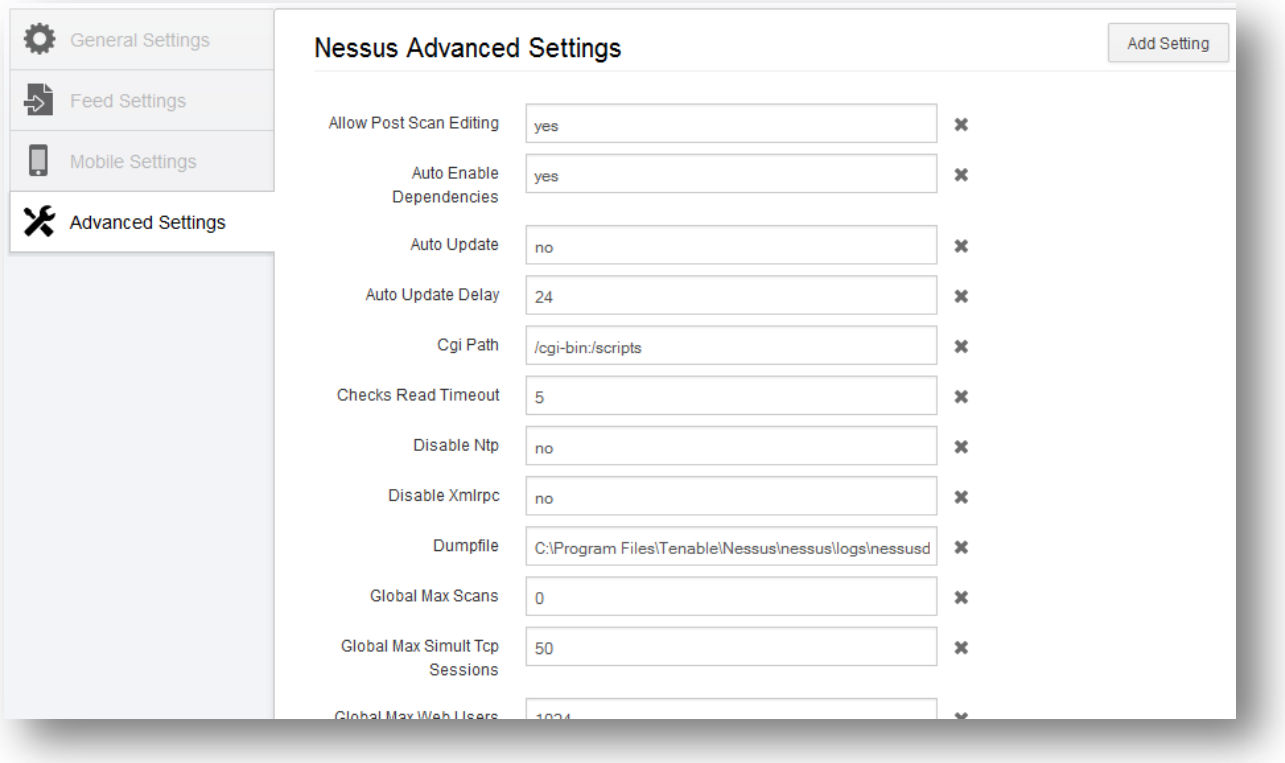
A seção “Offline Update” permite especificar um arquivo de plugin para processamento. Para obter mais detalhes sobre atualização off-line, consulte a seção “Nessus sem acesso à Internet” neste documento.

O uso do cliente legado por meio do protocolo NTP é suportado pelo Nessus 5, mas está disponível apenas para os clientes do ProfessionalFeed.

Opções de configuração avançadas

O Nessus utiliza uma grande variedade de opções de configuração que oferecem um controle mais granular sobre o funcionamento do scanner. Na guia “Advanced” (Avançado), opção “Configuration” (Configuração), o usuário administrador pode controlar essas configurações.

ATENÇÃO: Quaisquer alterações na configuração do scanner Nessus afetarão **TODOS** os usuários do Nessus. Edite esta opção com cuidado!



Cada opção pode ser configurada ao editar o campo correspondente e clicar no botão “Save” (Salvar) na parte inferior da tela. Além disso, a opção pode ser removida completando ao clicar no botão ✖.

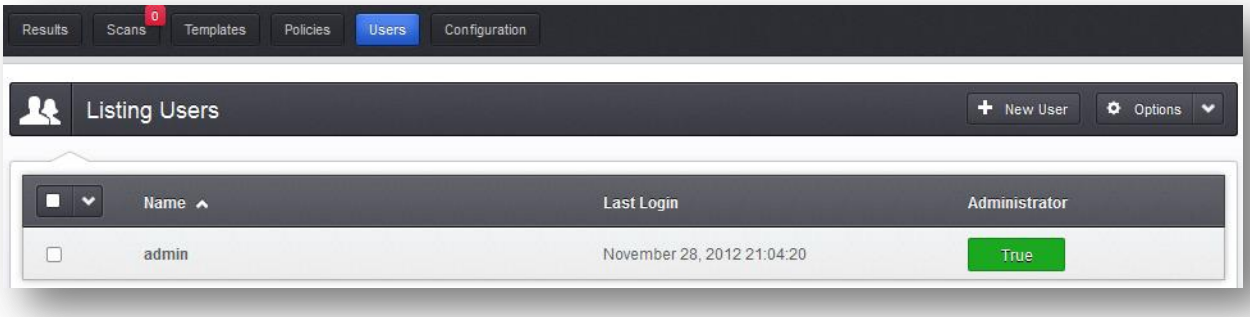
Normalmente, a GUI (interface do usuário) Nessus funciona na porta 8834. Para alterar a porta, edite **`xmlrpc_listen_port`** com a porta desejada. O servidor Nessus processará a alteração em alguns minutos.

Se outras preferências forem necessárias, clique no botão “**Add Preference Item**” (Adicionar item de preferência), digite o nome e o valor e pressione “**Save**” (Salvar). Depois de a preferência ser atualizada e salva, o Nessus processará as alterações no intervalo de alguns minutos.

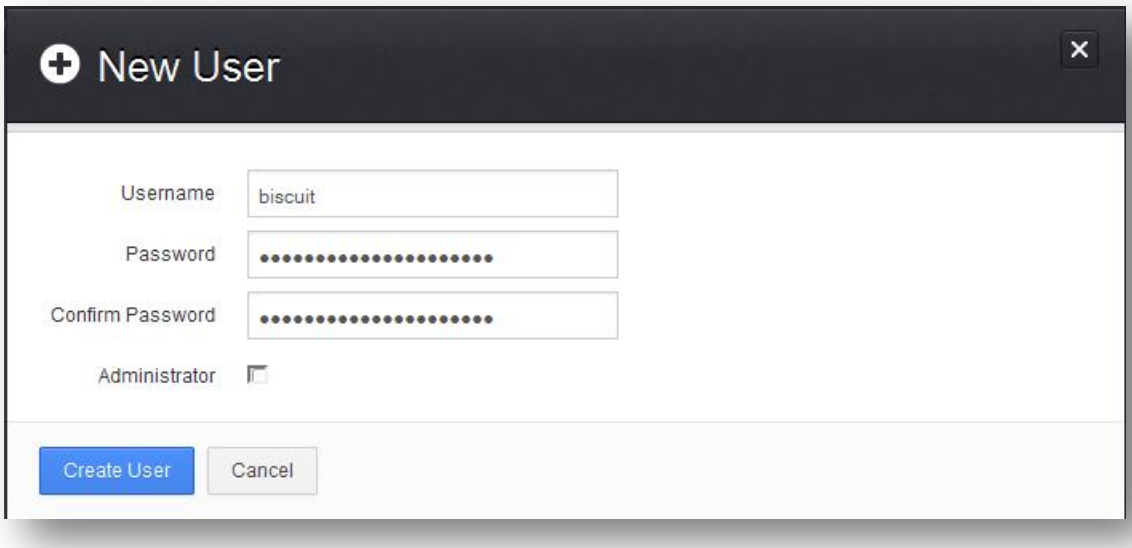
Para obter mais detalhes sobre as opções de configuração, consulte a seção “Configuração do daemon do Nessus (usuários avançados)” neste documento.

Criação e gerenciamento de usuários do Nessus

Durante a configuração inicial, um usuário administrativo é criado. Usando as credenciais especificadas durante a instalação, faça login na GUI (interface do usuário) Nessus. Depois de autenticado, clique no cabeçalho “Users” (Usuários) na parte superior:

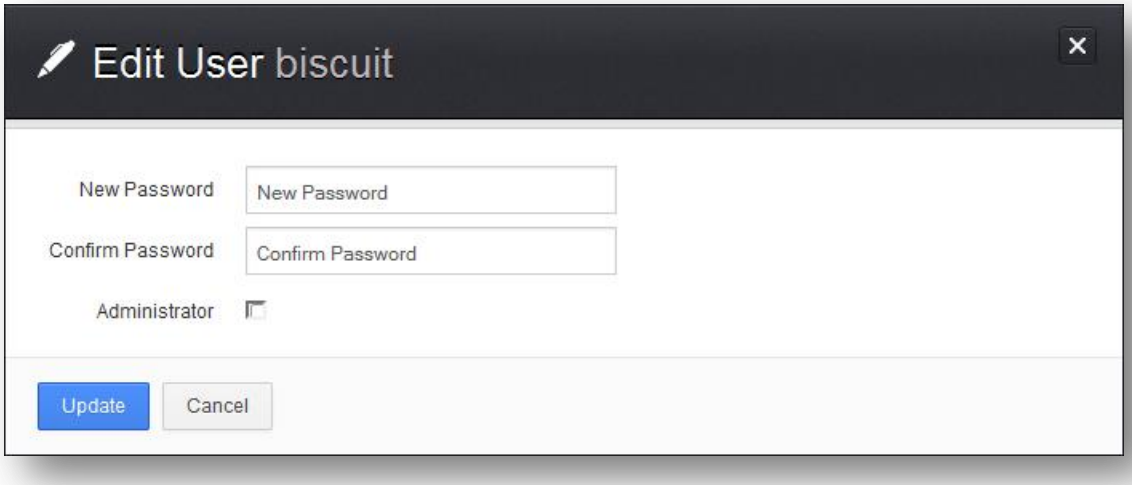


Para criar um novo usuário, clique em "**New User**" (Novo usuário) no canto superior direito. Isto abrirá uma caixa de diálogo solicitando os detalhes necessários:



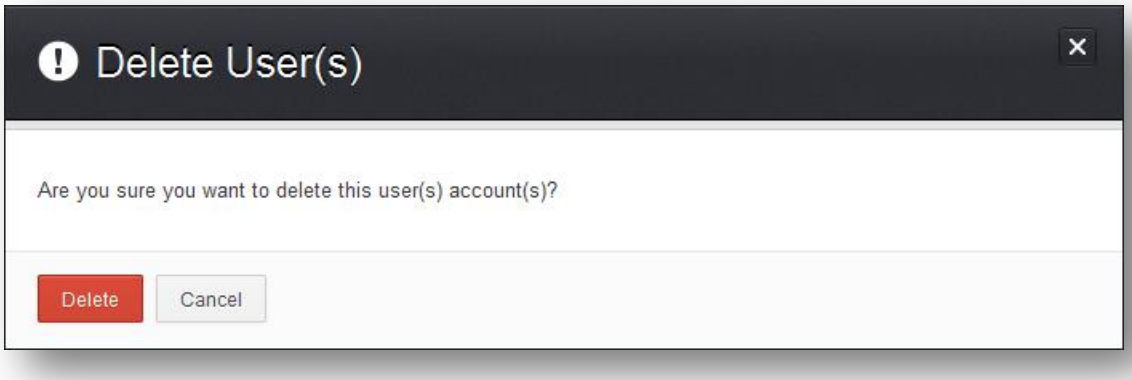
Digite o nome de usuário e a senha, confirme a senha e determine se o usuário deve ter privilégios de administrador.

Se a conta do usuário precisar ser alterada, clique duas vezes no usuário:



Não é possível renomear um usuário. Para alterar o nome de um usuário, exclua o usuário e crie um novo usuário com o nome de login apropriado.

Para remover o usuário, marque a caixa de seleção ao lado da conta na lista, selecione “Options” (Opções) no alto à direita, clique em “Delete User” (Excluir usuário) e confirme:



Um usuário não administrador não pode fazer upload de plugins para o Nessus, não pode reiniciá-lo remotamente (necessário depois do upload do plugin) e não pode substituir a definição de `max_hosts/max_checks` na seção de configuração. **Se o usuário for usado pelo SecurityCenter, deve ser um usuário administrador.** O SecurityCenter mantém a sua própria lista de usuários e define permissões para eles.

Se for necessário atribuir restrições a uma conta de usuário do Nessus, isso pode ser feito com a interface de linha de comando (CLI), conforme descrito na seção “Como usar e gerenciar o Nessus a partir da linha de comando” neste documento.

Configuração do daemon do Nessus (usuários avançados)

O menu de configuração da GUI (interface do usuário) Nessus contém várias opções configuráveis. Por exemplo: o local com o número máximo de verificações e hosts examinados simultaneamente, os recursos que deseja que o **nessusd** utilize e a velocidade na qual os dados devem ser lidos, além de várias outras opções. Recomenda-se que as definições ser verificadas e alteradas de forma adequada com base no seu ambiente de varredura. A lista completa de opções de configuração é explicada no final desta seção.

Os valores de **max_hosts** e **max_checks** podem, eventualmente, afetar muito a capacidade do sistema Nessus de realizar varreduras, bem como dos sistemas que estão sendo examinados em busca de vulnerabilidades na rede. Preste especial atenção a esses dois parâmetros.

As duas configurações e seus valores padrão conforme visualizados no menu de configuração estão disponíveis a seguir:

Opção	Valor
max_hosts	40
max_checks	5

Observe que essas configurações são substituídas a cada varredura quando for utilizado o SecurityCenter da Tenable ou uma política personalizada na interface do usuário Nessus. Para exibir ou modificar essas opções em um modelo de varredura no SecurityCenter, edite as “Scan Options” (Opções de Varredura) de Scan Template. Na interface do usuário Nessus, edite a política de varredura e clique em na guia “Options” (Opções).

Observe que o parâmetro **max_checks** tem um limite codificado de 15. Qualquer valor acima de 5 causará efeitos adversos frequentes, pois a maioria dos servidores não consegue processar tantas solicitações intrusivas ao mesmo tempo.

Observações sobre max_hosts:

Como o nome indica, este é o número máximo de sistemas de destino que serão verificados a qualquer momento. Quanto maior o número de sistemas examinados simultaneamente por um único scanner Nessus, mais recursos da RAM, do processador e da largura de banda da rede do sistema de varredura serão consumidos. Ao definir o valor de **max_hosts**, deve-se levar em consideração a configuração de hardware do sistema de varredura e outros aplicativos em execução.

Uma vez que vários outros fatores específicos do seu ambiente de varredura também afetarão suas varreduras com o Nessus (por exemplo: a política de varredura da sua organização, outros tráfegos de rede, o efeito um tipo particular de varredura sobre os hosts submetidos à varredura), a experiência indicará a configuração ideal de **max_hosts**.

Um ponto de partida convencional para determinar a melhor configuração de **max_hosts** em um ambiente corporativo consiste em defini-lo como “20” em um sistema Nessus em Unix, e “10” em um scanner Nessus no Windows.

Observações sobre max_checks:

Este é o número de verificações simultâneas ou plugins que será executado em um único host de destino durante uma varredura. Observe que um ajuste muito alto deste número pode sobrecarregar os sistemas examinados, dependendo dos plugins usados na varredura.

Multiplique **max_checks** por **max_hosts** para encontrar o número de verificações simultâneas que podem ser executadas a qualquer momento durante uma varredura. Uma vez que **max_checks** e **max_hosts** são usados em conjunto, o ajuste de **max_checks** muito elevado também pode causar limitações de recursos em um sistema de

varredura Nessus. Da mesma maneira que o **max_hosts**, a experiência indicará a configuração ideal de **max_checks**, mas recomenda-se que esse ajuste seja sempre relativamente baixo.

Opções de configuração

A tabela a seguir fornece uma breve explicação sobre cada opção de configuração disponível no menu de configuração. Muitas dessas opções são configuráveis por meio da interface do usuário ao criar uma política de varredura.

Opção	Descrição
auto_enable_dependencies	Ativa automaticamente os plugins dos quais depende. Se estiver desativado, nem todos os plugins poderão ser executados, mesmo se estiverem selecionados em uma política de varredura.
auto_update	Atualizações automáticas de plugins. Se estiver ativado e o Nessus registrado, localize os plugins mais recentes em plugins.nessus.org automaticamente. Desative a opção se o scanner estiver em uma rede isolada sem acesso à Internet.
auto_update_delay	Número de horas de espera entre duas atualizações. Quatro (4) horas é o intervalo mínimo permitido.
cgi_path	Durante os testes dos servidores da Web, use esta lista de caminhos de CGI delimitada por dois pontos.
checks_read_timeout	Limite de tempo de leitura nos soquetes dos testes.
disable_ntp	Desativa o protocolo NTP anterior.
disable_xmlrpc	Desativa a nova interface XMLRPC (servidor da Web).
dumpfile	Localização de um arquivo de despejo do resultado de uma depuração, se for gerado.
enable_listen_ipv4	Instrui o Nessus a escutar em IPv4.
enable_listen_ipv6	Instrui o Nessus a escutar em IPv6, caso o sistema reconheça endereços IPv6.
global.max_scans	Se o valor for diferente de zero, define o número máximo de varreduras que podem ocorrer em paralelo. **Nota**: Se esta opção não for usada, nenhum limite será imposto.
global.max_simult_tcp_ sessions	Número máximo de sessões TCP simultâneas entre todas as varreduras. **Nota**: Se esta opção não for usada, nenhum limite será imposto.
global.max_web_users	Se o valor for diferente de zero, define o máximo de usuários (da Web) que podem se conectar em paralelo. **Nota**: Se esta opção não for usada, nenhum limite será imposto.
host.max_simult_tcp_ sessions	Número máximo de sessões TCP simultâneas por host examinado.
listen_address	Endereço IPv4 para "escutar" as conexões de entrada. Se for definido como 127.0.0.1, limitará o acesso às conexões locais somente.
listen_port	Porta de escuta (antigo protocolo NTP). Usado para conexões anteriores à versão 4.2 do NessusClient.

log_whole_attack	Registro de todos os detalhes do ataque? Usado para depurar problemas na varredura, mas isso pode consumir muito recursos do disco.
logfile	Local em que o arquivo de log do Nessus é armazenado.
max_hosts	Número máximo de hosts verificados ao mesmo tempo durante uma varredura.
max_checks	Número máximo de controles simultâneos verificados em cada host testado.
max_simult_tcp_sessions	Número máximo de sessões TCP simultâneas por varredura.
nasl_log_type	Instrui o tipo de resultado do mecanismo NASL em **`nessusd.dump`**.
nasl_no_signature_check	O Nessus deve considerar todos os scripts NASL como assinados? A seleção da opção “yes” (sim) não é segura e não recomendável.
nessus_syn_scanner. global_throughput.max	Define o número máximo de pacotes síncronos que o Nessus enviará por segundo durante sua varredura de portas (independentemente de quantos hosts sejam examinados ao mesmo tempo). Ajuste esta configuração de acordo com a sensibilidade do dispositivo remoto a um grande número de pacotes syn.
non_simult_ports	Portas nas quais dois plugins não devem ser executados simultaneamente.
optimize_test	Otimiza o procedimento de teste. A alteração desta a opção para “no” (não) fará com que as varreduras demorem mais e, portanto, gere mais falsos positivos.
paused_scan_timeout	Interrompe uma varredura suspensa após ‘n' minutos (0 = nenhum tempo limite).
plugin_upload	Designa se os usuários administradores podem fazer upload de plugins.
plugin_upload_suffixes	Sufixos dos plugins que os usuários administradores podem enviar (upload).
plugins_timeout	Duração máxima da atividade de um plugin (em segundos).
port_range	Intervalo de portas a ser examinado pelos scanners. É possível usar as palavras-chaves “default” (padrão) ou “all” (todo), além de uma lista de portas delimitada por vírgulas ou intervalos de portas.
purge_plugin_db	Determina se o Nessus deve remover o banco de dados de plugins a cada atualização. Instrui o Nessus a remover, baixar novamente e reconstruir o banco de dados do plugin para cada atualização. A seleção da opção “yes” (sim) fará com que cada atualização seja consideravelmente mais lenta.
qdb_mem_usage	Instrui o Nessus a usar mais ou menos memória quando estiver ocioso. Se o Nessus for instalado em um servidor dedicado, o ajuste desta opção como “high” (alto) irá requerer mais memória para aumentar o desempenho. Se o Nessus for instalado em um computador compartilhado, o ajuste desta opção como “low” (baixo) consumirá menos memória, no entanto, o desempenho será afetado de maneira relativa.
reduce_connections_on_ congestion	Reduz o número de sessões TCP simultâneas quando a rede parece estar congestionada.

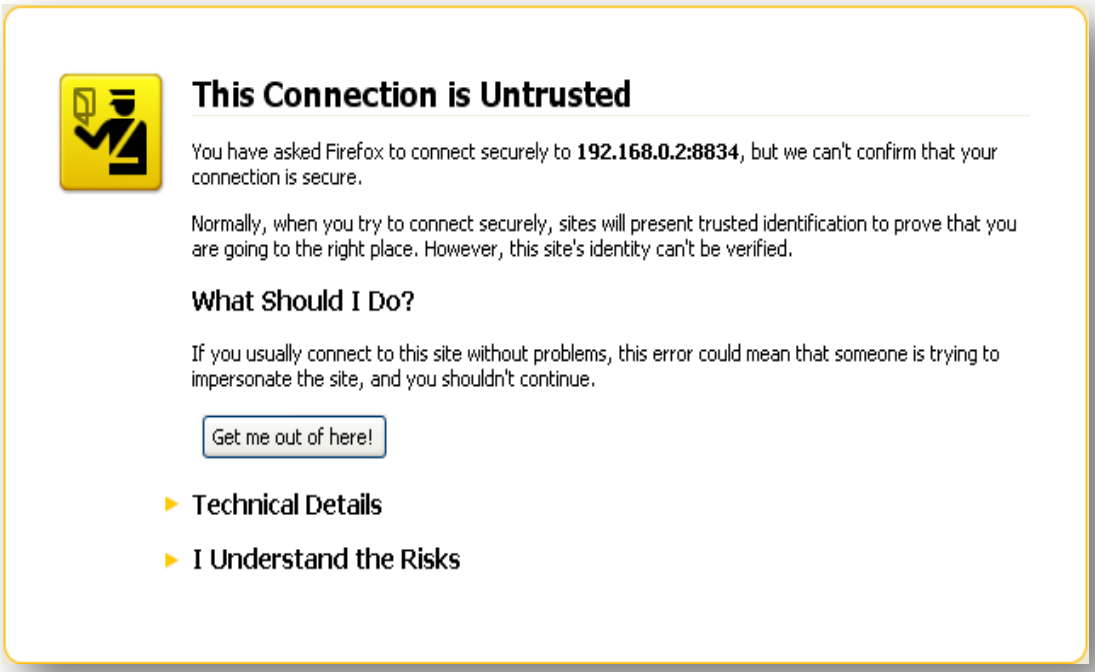
report_crashes	Informar quaisquer falhas à Tenable de maneira anônima?
rules	Localização do arquivo de regras do Nessus (nessusd.rules).
safe_checks	As verificações seguras dependem da captura de um banner e não de testes ativos de uma vulnerabilidade.
save_knowledge_base	Salva o banco de dados de conhecimento em disco para uso posterior.
silent_dependencies	Se estiver ativado, a lista de dependências de plugins e seus resultados não irão figurar no relatório. Um plugin pode ser selecionado como parte de uma política que depende que outros plugins sejam executados. Normalmente, o Nessus executará as dependências do plugin, mas não incluirá a saída no relatório. A definição desta opção como no (não) fará com que tanto o plugin selecionado quanto todas as dependências do plugin apareçam no relatório.
slice_network_addresses	Se esta opção for ativada, o Nessus, não examinará uma rede de forma incremental (10.0.0.1, 10.0.0.2, 10.0.0.3 e assim por diante), mas tentará dividir a carga de trabalho por toda a rede (por exemplo: verificará 10.0.0.1, depois 10.0.0.127, depois 10.0.0.2, depois 10.0.0.128 e assim por diante).
source_ip	Em caso de um sistema de vários homes com IPs diferentes na mesma sub-rede, esta opção informa ao scanner Nessus a placa de rede/IP que deve ser usada nos testes. Se forem fornecidos vários IPs, o Nessus os percorrerá sempre que efetuar uma conexão.
ssl_cipher_list	Apenas criptografias SSL “fortes” devem ser usadas na conexão com a porta 1241. Permite o uso da palavra-chave “forte” ou das designações OpenSSL gerais indicadas em http://www.openssl.org/docs/apps/ciphers.html.
stop_scan_on_disconnect	Interrompe a varredura de um host desconectado durante a varredura.
stop_scan_on_hang	Interrompe uma varredura possivelmente suspensa.
throttle_scan	Controla a velocidade da varredura em caso de sobrecarga da CPU.
use_kernel_congestion_detection	Usa mensagens de congestionamento de TCP do Linux para reduzir a escala de atividade de varredura, se necessário.
www_logfile	Local em que o log do Nessus Web Server (interface do usuário) é armazenado.
xmlrpc_idle_session_timeout	Desconexão de sessão ociosa do XMLRPC (em minutos).
xmlrpc_import_feed_policies	Se o valor for “no” (não), o Nessus não incluirá políticas padrão de varredura fornecidas pela Tenable.
xmlrpc_listen_port	Porta de escuta do Nessus Web Server (novo protocolo XMLRPC).
xmlrpc_min_password_len	Instrui o Nessus a aplicar uma política de comprimento de senha para os usuários do scanner.

O valor padrão de **`report_crashes`**, e ·yes” (Sím). As informações relacionadas a uma falha no Nessus serão enviadas à Tenable para ajudar a depurar problemas e oferecer o software da mais alta qualidade. Nenhuma informação de

identificação pessoal ou do sistema é enviada. Essa configuração pode ser substituída por “no” (não) por um usuário Nessus admin.

Configuração do Nessus com certificado SSL personalizado

A instalação padrão do Nessus utiliza um certificado SSL autoassinado. Ao usar a interface da Web para acessar o scanner Nessus pela primeira vez, o navegador exibirá um erro indicando que o certificado não é confiável:


This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.2:8834, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

Para evitar avisos do navegador, pode ser usado um certificado SSL personalizado específico da sua organização. Durante a instalação, o Nessus cria dois arquivos que compõem o certificado: **`servercert.pem`** e **`serverkey.pem`**. Esses arquivos devem ser substituídos por arquivos de certificados gerados por sua organização ou uma autoridade de certificação confiável (CA).

Antes de substituir os arquivos de certificado, interrompa o servidor Nessus. Substitua os dois arquivos e reinicie o servidor Nessus. As conexões subsequentes com o scanner não devem exibir um erro se o certificado tiver sido gerado por uma CA confiável.

A tabela a seguir lista a localização dos arquivos de certificados, conforme o sistema operacional:

Sistema operacional	Locais dos arquivos de certificação
Linux e Solaris	`/opt/nessus/com/nessus/CA/servercert.pem` `/opt/nessus/var/nessus/CA/serverkey.pem`
FreeBSD	`/usr/local/nessus/com/nessus/CA/servercert.pem` `/usr/local/nessus/var/nessus/CA/serverkey.pem`
Windows	`C:\Program Files\Tenable\Nessus\nessus\CA\`

Mac OS X	**/Library/Nessus/run/com/nessus/CA/servercert.pem** **/Library/Nessus/run/var/nessus/CA/serverkey.pem**

O Nessus 5 oferece suporte a cadeias de certificados SSL.

É possível também visitar `https://[IP address]:8834/getcert` para instalar a CA de raiz no seu navegador. Isto removerá o aviso.

Para configurar uma cadeia de certificados intermediários, um arquivo denominado **serverchain.pem** deve ser colocado no mesmo diretório do arquivo **servercert.pem**. O arquivo deve conter os certificados 1-n intermediários (certificados públicos concatenados) necessários para a construção da cadeia de certificados completa do servidor Nessus para o certificado raiz atual (confiável pelo navegador do usuário).

Autenticação do Nessus com certificado SSL

Autenticação de certificado de cliente SSL

O Nessus permite aos usuários utilizar a autenticação de certificado de cliente SSL. Isso permite o uso de certificados de cliente SSL, cartões inteligentes e autenticação CAC quando o navegador estiver configurado para este método.

O Nessus oferece métodos de autenticação de certificados SSL baseados em senha ou SSL para contas de usuário. Ao criar um usuário para autenticação de certificados SSL, o utilitário **nessus-mkcert-client** pode ser usado através da linha de comando no servidor Nessus.

Configurar o Nessus para certificados

O primeiro passo para permitir a autenticação de certificados SSL consiste em configurar o servidor da Web da Nessus com um certificado de servidor e CA. Este processo permite que o servidor da Web aceite os certificados criados pela Autoridade de Certificação (CA) para fins de autenticação. Os arquivos gerados relativos aos certificados devem pertencer a `root:root` e as permissões padrão devem ser satisfatórias.

1. Crie um novo CA personalizado e certificado de servidor para o servidor Nessus com o comando **nessus-mkcert** na linha de comando (opcional). Isto colocará os certificados em seus diretórios corretos.

Quando for solicitado o nome do host, digite o nome DNS ou endereço IP do servidor no navegador, por exemplo: https://hostname:8834/ ou https://ipaddress:8834/. O certificado padrão usa o hostname.

2. Se o certificado CA for usado em vez dos Nessus gerado, faça uma cópia do certificado CA autoassinado com o comando apropriado para o sistema operacional:

   Unix/Linux:
   # cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/ORIGcacert.pem

   Windows:
   C:\> copy \Program Files\Tenable\Nessus\Nessus\CA\cacert.pem C:\Program Files\Tenable\Nessus\nessus\CA\ORIGcacert.pem

3. Se os certificados a serem usado para autenticação forem criados por um CA que não seja o servidor Nessus, o certificado CA deverá ser instalado no servidor Nessus:

   Unix/Linux:
   Copie o certificado CA da organização em **/opt/nessus/com/nessus/CA/cacert.pem**

   Windows:
   Copie o certificado CA da organização em **C:\Program Files\Tenable\Nessus\Nessus\CA\cacert.pem**

4. Configure o servidor Nessus para autenticação de certificado. Uma vez que a autenticação de certificado seja ativada, o login com o nome de usuário e a senha será desativado.

   Unix/Linux:
   `# /opt/nessus/sbin/nessus-fix --set force_pubkey_auth=yes`

   Windows:
   `C:\> \program files\Tenable\Nessus\nessus-fix --set force_pubkey_auth=yes`

5. Com o CA no lugar e a definição de **`force_pubkey_auth`** ativada, reinicie o serviço Nessus com o comando **`service nessusd restart`**.

Depois de configurar o Nessus com o(s) certificado(s) CA apropriados, os usuários podem fazer login no Nessus usando certificados de cliente SSL, "Smart Cards" (cartões inteligentes) e CACs.

Criar certificados SSL do Nessus para login

Para fazer o login em um servidor Nessus com certificados SSL, os certificados devem ser criados com o utilitário. Para esse processo, o utilitário de linha de comando **`nessus-mkcert-client`** deve ser usado no sistema. As seis perguntas são feitas para definir padrões para a criação de usuários durante a sessão atual. As perguntas incluem tempo de vida do certificado, país, estado, localização, organização e unidade organizacional. Os padrões para estas opções podem ser alteradas durante a criação do usuário, se desejar. O(s) usuário(s) será(ão) criado(s) individualmente, conforme solicitado. Ao término do processo, os certificados são copiados de forma apropriada e usados para acesso ao servidor Nessus.

1. No servidor Nessus, execute o comando **`nessus-mkcert-client.`**

   Unix/Linux:
   `# /opt/nessus/sbin/nessus-mkcert-client`

   Windows (executar como usuário administrador local):
   `C:\> \Program Files\Tenable\Nessus\nessus-mkcert-client`

2. Preencha os campos quando solicitado. O processo é idêntico no servidor Linux/Unix ou Windows.

```
Do you want to register the users in the Nessus server as soon as you create their
       certificates ? [n]: y

-------------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]: MD
Your location (e.g. town) [New York]: Columbia
Your organization []: Content
Your organizational unit []: Tenable
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a
       single dot '.'
*********
User #1 name (e.g. Nessus username) []: squirrel
Should this user be administrator?  [n]: y
Country (two letter code) [US]:
```

```
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Content]:
Organizational unit [Tenable]:
e-mail []:

User rules
----------
nessusd has a rules system which allows you to restrict the hosts that firstuser has
       the right to test. For instance, you may want him to be able to scan his own
       host only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
Another client certificate?  [n]:
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
You will have to copy them by hand
```

Os certificados de cliente serão criados em um diretório temporário randomizado apropriado para o sistema. O diretório temporário será identificado com a linha que começa com “Your client certificates are in” (Seus certificados de cliente estão em).

3. Haverá dois arquivos criados no diretório temporário: **cert_squirrel.pem** e **key_squirrel.pem**. Esses arquivos devem ser combinados e exportados para um formato que pode ser importado para o navegador, como **.pfx**. Isto pode ser feito com o programa **openssl** e o comando a seguir:

   ```
   # openssl pkcs12 -export -out combined_squirrel.pfx –inkey
   key_squirrel.pem -in cert_squirrel.pem -chain -CAfile
   /opt/nessus/com/nessus/CA/cacert.pem -passout pass:'SecretWord' -name 'Nessus User
   Certificate for: squirrel'
   ```

   O arquivo **combined_squirrel.pfx** resultante será criado no diretório do qual o comando é lançado. Este arquivo deve ser importado para o armazenamento de certificados pessoais no navegador.

Ativar conexões com cartão inteligente ou cartão CAC

Uma vez que o CAcert para o cartão inteligente, CAC ou dispositivo similar seja ativado, os usuários correspondentes devem ser criados para corresponder ao Nessus. Durante o processo, os usuários criados devem corresponder ao CN do cartão que será usado pelo usuário para se conectar.

1. No servidor Nessus, execute o comando **nessus-mkcert-client.**

   Unix/Linux:
   # /opt/nessus/sbin/nessus-mkcert-client

   Windows (executar como usuário administrador local):
   C:\> \Program Files\Tenable\Nessus\nessus-mkcert-client.exe

2. Preencha os campos quando solicitado. O processo é idêntico no servidor Linux/Unix ou Windows. O nome do usuário deve corresponder ao CN fornecido pelo certificado no cartão.

```
Do you want to register the users in the Nessus server as soon as you create their
      certificates ? [n]: y

--------------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
--------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]: MD
Your location (e.g. town) [New York]: Columbia
Your organization []: Content
Your organizational unit []: Tenable
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a
      single dot '.'
*********
User #1 name (e.g. Nessus username) []: squirrel
Should this user be administrator?  [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Content]:
Organizational unit [Tenable]:
e-mail []:

User rules
----------
nessusd has a rules system which allows you to restrict the hosts that firstuser has
      the right to test. For instance, you may want him to be able to scan his own
      host only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
Another client certificate?  [n]:
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
You will have to copy them by hand
```

Os certificados de cliente serão criados em um diretório temporário randomizado apropriado para o sistema. O diretório temporário será identificado com a linha que começa com “Your client certificates are in”. Para o uso de autenticação de cartão, esses certificados não são necessários e podem ser excluídos.

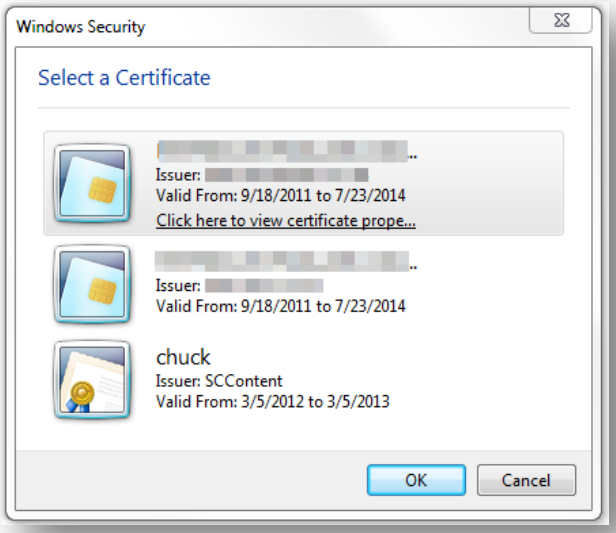
3. Uma vez criado, o usuário com o cartão adequado pode acessar o servidor Nessus e autenticar-se automaticamente quando o PIN ou segredo semelhante for fornecido.

Conexão com certificado ou navegador ativado com cartão

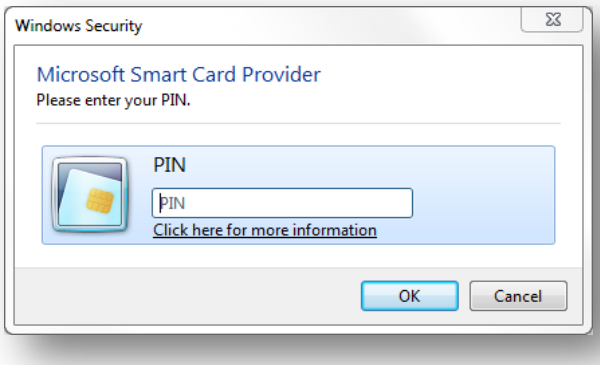
As informações a seguir são fornecidas considerando que o navegador esteja configurado para a autenticação de certificado SSL. Isto inclui o CA confiável e adequado no navegador. Consulte os arquivos de ajuda do navegador ou outra documentação para configurar este recurso.

O processo de login do certificado começa quando o usuário se conecta ao Nessus.

1. Abra o navegador e navegue até o servidor Nessus.
2. O navegador apresentará uma lista de identidades de certificados disponíveis para seleção:



3. Após selecionar o certificado, o prompt para o PIN ou a senha do o certificado será exibido (se necessário) para acesso ao certificado. Se o PIN ou a senha forem digitados corretamente, o certificado estará disponível para a sessão atual com o Nessus.



4. Ao navegar pela interface da Web do Nessus, o usuário poderá visualizar brevemente o nome de usuário e a senha na tela, seguidos por um login automático como o usuário designado. A interface do usuário Nessus pode ser usada normalmente.

Ao sair da sessão, a tela de login padrão do Nessus será exibida. Para se conectar novamente com o mesmo certificado, atualize o navegador. Caso seja necessário usar outro certificado, reinicie a sessão do navegador.

Nessus sem acesso à Internet

Esta seção descreve as etapas para registrar o scanner Nessus, instalar o Activtion Code (Código de Ativação) e receber os plugins atualizados quando o sistema Nessus não tiver acesso direto à Internet.

Os Activation Codes (Códigos de Ativação) obtidos por meio do processo off-line descrito a seguir estão vinculados ao scanner Nessus usado durante o processo de atualização off-line. Não é possível usar o pacote de plugins baixado com outro scanner Nessus.

Comece seguindo as instruções fornecidas pelo Nessus. Quando solicitar um Activation Code (Código de Ativação), digite “Offline” conforme as instruções.

Como gerar um código de confirmação

É possível obter o Activtion Code (Código de Ativação) da assinatura do Nessus ao acessar a conta do Tenable Support Portal para o ProfessionalFeed ou pelo e-mail de registro do HomeFeed.

Observe que só é possível usar um Activtion Code (Código de Ativação) por scanner, a menos que os scanners sejam gerenciados pelo SecurityCenter.

Ao receber o Activtion Code (Código de Ativação), execute o seguinte comando no sistema no qual o Nessus está instalado:

Windows:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --challenge
```

Linux e Solaris:

```
# /opt/nessus/bin/nessus-fetch --challenge
```

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --challenge
```

Mac OS X:

```
# /Library/Nessus/run/bin/nessus-fetch --challenge
```

Isso produzirá uma string chamada “challenge code” (código de confirmação), que tem o seguinte formato:

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Como obter e instalar plugins atualizados

Em seguida, acesse https://plugins.nessus.org/offline.php, copie e cole nas respectivas caixas de texto o string “challenge” (confirmação) e o Activtion Code (Código de Ativação) recebido:

Isto produzirá um URL parecida com a captura de tela abaixo:

A tela dá acesso ao download do feed mais recente de plugins do Nessus (**`all-2.0.tar.gz`**), junto com um link para o arquivo **`nessus-fetch.rc`** na parte inferior da tela.

Salve a URL, pois será usada sempre que os plugins forem atualizados, conforme descrito a seguir.

Um código de registro usado para atualizações offline não pode ser usado no mesmo servidor do scanner Nessus através do Nessus Server Manager.

Caso seja necessário confirmar o código de registro de um determinado scanner, pode-se usar a opção **`--code-in-use`** para o programa **`nessus-fetch`**.

Copie o arquivo **`nessus-fetch.rc`** no host em que o Nessus está instalado, no seguinte diretório:

Windows:
`C:\Program Files\Tenable\Nessus\conf`

Linux e Solaris:
`/opt/nessus/etc/nessus/`

FreeBSD:
`/usr/local/nessus/etc/nessus/`

Mac OS X:
`/Library/Nessus/run/etc/nessus/`

O arquivo **`nessus-fetch.rc`** deve ser copiado apenas uma vez. Os downloads subsequentes dos plugins do Nessus devem ser copiados para o diretório apropriado a cada vez, conforme descrito a seguir.

Observe que, normalmente, o Nessus tentará atualizar os plugins a cada 24 horas após o registro. Se não desejar que a atualização on-line seja feita, defina a opção "**`auto_update`**" (atualização_automática) como "**`no`**" (não) no menu "**Configuration**" (Configuração) -> "**Advanced**" (Avançado).

Execute esta etapa sempre que realizar uma atualização offline dos plugins.

Após o download, mova o arquivo **`all-2.0.tar.gz`** para o diretório do Nessus. Em seguida, instrua o Nessus a processar o arquivo de plugins:

Windows:
`C:\Program Files\Tenable\Nessus>`**`nessus-update-plugins.exe all-2.0.tar.gz`**

Unix (modifique o caminho para a sua instalação):
`#` **`/opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz`**

Após o processamento, será necessário reiniciar o Nessus para que as alterações sejam efetivadas. Consulte as seções "Manipulação do serviço Nessus por meio de CLI do Windows" ou "Como iniciar/parar o daemon do Nessus" (Unix) para obter detalhes sobre como reiniciar.

Depois de instalar o plugins, o arquivo **`all-2.0.tar.gz`** poderá ser removido. No entanto, a Tenable recomenda manter a versão mais recente do arquivo de plugin baixado caso seja necessário novamente.

Com isso, os plugins mais recentes estarão disponíveis. Sempre que quiser atualizar os plugins quando não tiver acesso à Internet, acesse a URL fornecida, obtenha o arquivo **tar/gz**, copie-o no sistema em que o Nessus está instalado e repita o processo acima.

Como usar e gerenciar o Nessus a partir da linha de comando

Diretórios principais do Nessus

A tabela a seguir indica o local de instalação e os diretórios principais usados pelo Nessus no *nix/Linux:

Diretório inicial do Nessus	Subdiretórios do Nessus	Objetivo
Distribuições do Unix		
Red Hat, SuSE, Debian, Ubuntu, Solaris: `/opt/nessus`	`./etc/nessus/`	Arquivos de configuração
	`./var/nessus/users/<username>/kbs/`	Banco de dados de conhecimento dos usuários salvo em disco
FreeBSD: `/usr/local/nessus`	`./lib/nessus/plugins/`	Plugins do Nessus
Mac OS X: `/Library/Nessus/run`	`./var/nessus/logs/`	Arquivos de log do Nessus

A tabela a seguir indica o local de instalação e os diretórios principais usados pelo Nessus no Windows:

Diretório inicial do Nessus	Subdiretórios do Nessus	Objetivo
Windows		
`\Program Files\Tenable\Nessus`	`\conf`	Arquivos de configuração
	`\data`	Modelos de folhas de estilo
	`\nessus\plugins`	Plugins do Nessus
	`\nessus\users\<username>\kbs`	Banco de dados de conhecimento dos usuários salvo em disco
	`\nessus\logs`	Arquivos de log do Nessus

Como criar e gerenciar usuários do Nessus com limitações de conta

O scanner Nessus é capaz de reconhecer uma disposição complexa de vários usuários. Por exemplo: diversas pessoas uma organização podem ter acesso ao mesmo scanner Nessus, mas com a capacidade de examinar intervalos IP diferentes, restringindo o acesso a alguns intervalos de IP restritos a pessoas autorizadas.

O exemplo a seguir destaca a criação de um segundo usuário do Nessus com autenticação por senha e regras que limitam o usuário à varredura de uma sub-rede classe B, 172.20.0.0/16. Para ver mais exemplos e a sintaxe das regras de usuários, consulte as páginas man **`nessus-adduser`**.

```
# /opt/nessus/sbin/nessus-adduser
Login                : tater-nessus
Login password :
```

```
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n)
       [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that tater-nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)
accept 172.20.0.0/16
deny 0.0.0.0/0



Login             : tater-nessus
Password: ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
accept 172.20.0.0/16
deny 0.0.0.0/0
Is that ok ? (y/n) [y] y
User added
```

Para visualizar a página man nessus-adduser(8), pode ser necessário, em alguns sistemas operacionais, executar os seguintes comandos:

```
# export MANPATH=/opt/nessus/man
# man nessus-adduser
```

Opções de linha de comando do Nessusd

Além de executar o servidor **nessusd**, várias outras opções de linha de comando podem ser usadas quando necessário. A tabela a seguir contém informações sobre esses vários comandos opcionais.

Opção	Descrição
-c <config-file>	Ao iniciar o servidor **nessusd**, esta opção é usada para especificar o arquivo de configuração **nessusd** do servidor a ser usado. Ele permite o uso de outro arquivo de configuração em vez do **/opt/nessus/etc/nessus/nessusd.db** padrão (ou **/usr/local/nessus/etc/nessus/nessusd.db** no FreeBSD).
-a <address>	Ao iniciar o servidor **nessusd**, esta opção é usada para instruir o servidor que "escute" apenas as conexões no endereço **<address>** que sejam um IP e não um nome de computador. Esta opção é útil ao executar o **nessusd** em um gateway e se o usuário não desejar que usuários externos se conectem ao **nessusd**.
-S <ip[,ip2,...]>	Ao iniciar o servidor **nessusd**, este comando força o IP de origem das conexões estabelecidas pelo Nessus durante a varredura de <ip>. Esta opção só será útil se o usuário tiver um computador com vários homes e endereços IP públicos que podem ser usados em vez do IP padrão. Para que esta configuração funcione, o host que

	executa o **nessusd** deve ter várias placas de rede com esses endereços IP definidos.
-p <port-number>	Ao iniciar o servidor **nessusd**, esta opção instrui o servidor que “escute” conexões do cliente na porta <port-number> em vez de escutar na porta 1241, que é a porta padrão.
-D	Ao iniciar o servidor **nessusd**, esta opção fará com que o servidor funcione em segundo plano (no modo daemon).
-v	Exibe o número da versão e desconecta.
-l	Exibe as informações sobre a licença do feed do plugin e desconecta.
-h	Mostra o resumo dos comandos e desconecta.
--ipv4-only	Escuta apenas o soquete IPv4.
--ipv6-only	Escuta apenas o soquete IPv6.
-q	Funciona no modo “silencioso” ao suprimir todas as mensagens enviadas a **stdout**.
-R	Força o reprocessamento dos plugins.
-t	Verifique a data e hora de cada plugin ao inicializar para compilar somente os plugins recém-atualizados.
-K	Define uma senha mestra para o scanner.

Se uma senha mestra for definida, o Nessus irá criptografar todas as políticas e credenciais contidas neles com a chave fornecida pelo usuário (mais segura que a chave padrão). Se uma senha for definida, a interface da Web solicitará a senha durante a inicialização.

ATENÇÃO: Se a senha mestra for definida e perdida, o administrador e o suporte da Tenable não poderão recuperá-la.

Um exemplo de uso é mostrado a seguir:

Linux:

```
# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a
<address>] [-S <ip[,ip,...]>]
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a
<address>] [-S <ip[,ip,...]>]
```

Manipulação do serviço Nessus por meio de CLI do Windows

O Nessus também pode ser iniciado a partir da linha de comando. Observe que a janela de comando deve ser aberta com privilégios de administrador:

```
C:\Windows\system32>net stop "Tenable Nessus"
The Tenable Nessus service is stopping.
The Tenable Nessus service was stopped successfully.


C:\Windows\system32>net start "Tenable Nessus"
The Tenable Nessus service is starting.
The Tenable Nessus service was started successfully.


C:\Windows\system32>
```

Como trabalhar como SecurityCenter

Descrição do SecurityCenter

O SecurityCenter da Tenable é um console de gerenciamento baseado na Web que unifica os processos de detecção de vulnerabilidades e de gerenciamento, gerenciamento de eventos e registros, monitoramento de conformidade e emissão de relatórios sobre todas as opções acima. O SecurityCenter permite a comunicação eficaz dos eventos de segurança com as equipes de TI, gestão e auditoria.

O SecurityCenter permite o uso de vários scanners Nessus em conjunto para realizar a varredura periódica de redes de praticamente qualquer porte. Com a API do Nessus (implementação personalizada do protocolo XML-RPC), o SecurityCenter se comunica com os scanners Nessus associados para enviar instruções de varredura e receber os resultados.

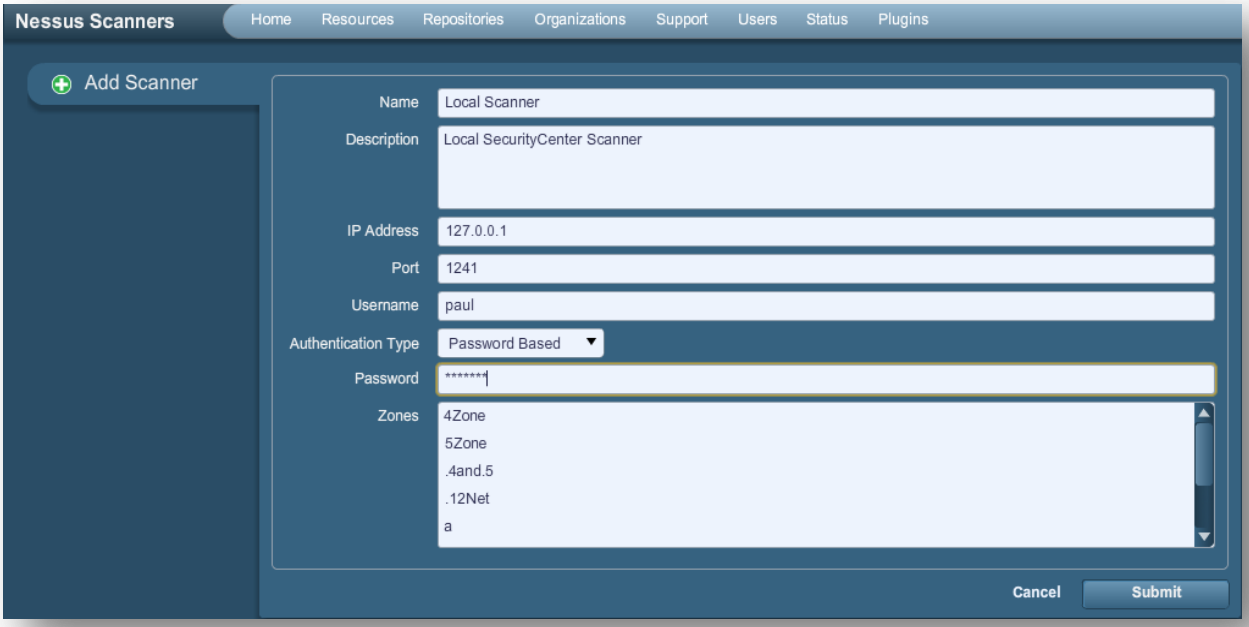
O SecurityCenter permite que aos usuários e administradores com diferentes níveis de segurança compartilhem informações sobre vulnerabilidades, organizem as vulnerabilidades por prioridade, visualizem os recursos de rede que apresentam problemas de segurança graves, façam recomendações para os administradores do sistema para a correção dos problemas de segurança e acompanhem o processo de correção das vulnerabilidades. O SecurityCenter recebe dados de diversos sistemas de detecção de intrusões principais, como o Snort e o ISS, por meio do Log Correlation Engine (Mecanismo de correlação de log).

O SecurityCenter também pode receber informações passivas sobre vulnerabilidades por meio do Passive Vulnerability Scanner da Tenable, de forma que os usuários finais possam descobrir novos hosts, aplicativos, vulnerabilidades e invasões sem a necessidade de realizar uma varredura ativa com o Nessus.

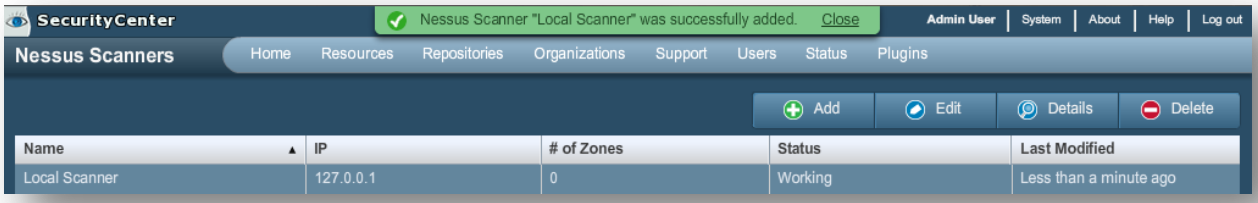
Configuração do SecurityCenter 4.0-4.2 para funcionar com o Nessus

O “Nessus Server” pode ser adicionado por meio da interface de administração do SecurityCenter. Usando essa interface, o SecurityCenter pode ser configurado para acessar e controlar praticamente qualquer scanner Nessus. Clique na guia “Resources” (Recursos) e, em seguida, clique em “**Nessus Scanners**”. Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “Add Scanner” (Adicionar Scanner). O endereço IP do scanner Nessus, a porta do Nessus (padrão: 1241), o ID de login administrativo, o tipo de autenticação e a senha (criada durante a configuração do Nessus) são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. Além disso, as zonas às quais o scanner Nessus será atribuído podem ser selecionadas.

Um exemplo de imagem da página “Add Scanner” do SecurityCenter é mostrado abaixo:



Depois de adicionar com êxito o scanner, a seguinte página é exibida após a seleção do scanner:

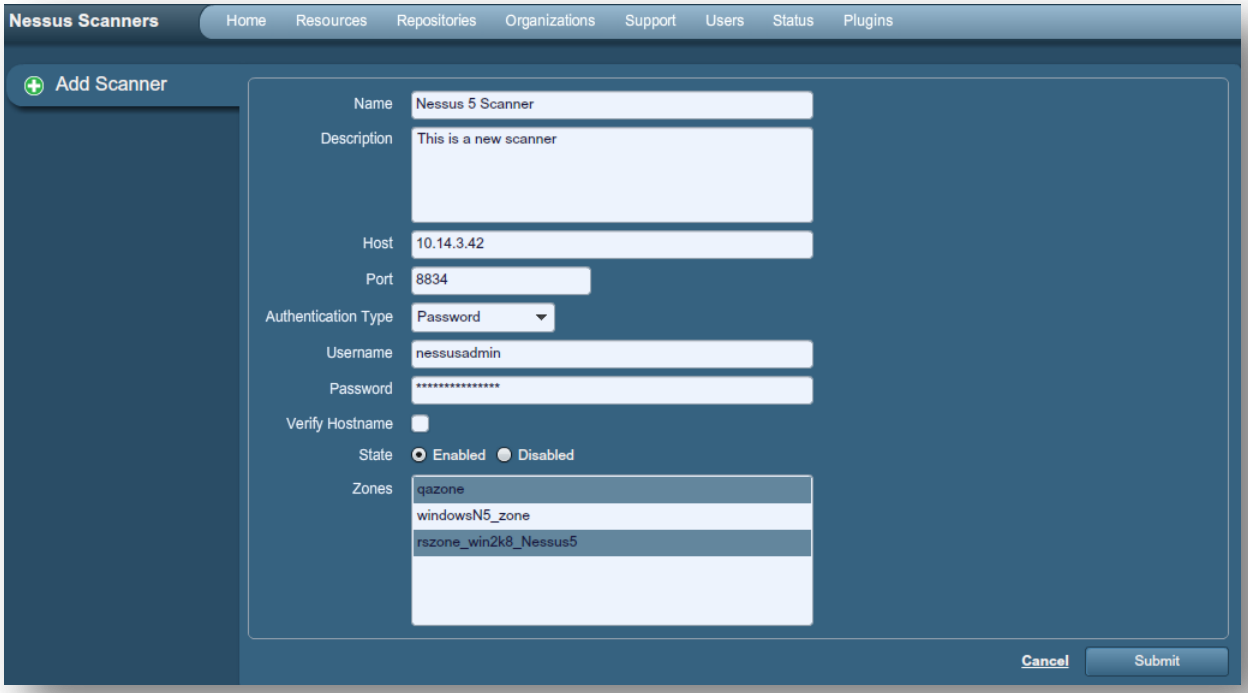


Consulte mais informações no “Guia de Administração do SecurityCenter”.

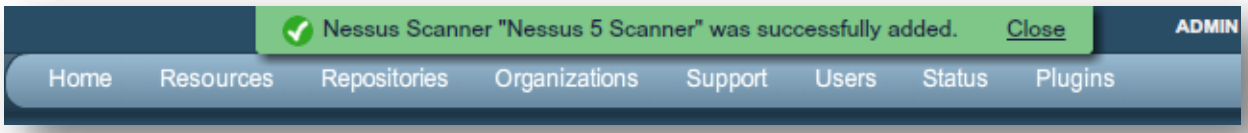
Configuração do SecurityCenter 4.4 para funcionar com o Nessus

A interface de administração do SecurityCenter é usada para configurar o acesso e controlar qualquer scanner Nessus, ou seja, versão 4.2.x ou superior. Clique na guia “**Resources**” (Recursos) e, em seguida, clique em “**Nessus Scanners**” (Scanners do Nessus). Clique em “**Add**” (Adicionar) para abrir a caixa de diálogo “**Add Scanner**” (Adicionar Scanner). O endereço IP ou nome do host do scanner Nessus, a porta do Nessus (padrão: 8834), as informações sobre o tipo de autenticação (criado durante a configuração do Nessus), a ID de login administrativo e a senha são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação “SSL Certificate” (Certificado SSL) for selecionada. A capacidade de verificar o nome do host é fornecida para verificação do CommonName (CN) do certificado SSL apresentado pelo servidor Nessus. O estado do scanner Nessus pode ser definido como ativado ou desativado, conforme o necessário (ativado é o padrão). As áreas do scanner Nessus podem ser atribuídas para seleção.

Um exemplo de imagem da página "**Add Scanner**" (Adicionar scanner) do SecurityCenter 4.4 é mostrado abaixo:



Depois de adicionar o scanner com êxito, o banner a seguir é exibido:



Para obter mais informações sobre como integrar o Nessus ao SecurityCenter, consulte "Guia de Administração do SecurityCenter".

Firewalls instalados no host

Se o servidor Nessus estiver configurado com um firewall local como ZoneAlarm, Sygate, BlackICE, firewall do Windows XP ou qualquer outro software de firewall, será necessário que as conexões sejam permitidas a partir do endereço IP do SecurityCenter.

Normalmente, a porta 8834 é usada. Nos sistemas Microsoft XP Service Pack 2 (SP2) e posteriores, clique em "**Security Center**" (Central de Segurança) no "**Control Panel**" (Painel de Controle) para gerenciar as configurações da opção "Firewall do Windows". Para abrir a porta 8834, selecione a guia "**Exceptions**" (Exceções) e adicione a porta "8834" à lista.

Se o SecurityCenter usar o protocolo NTP obsoleto por meio da porta 1241, os comandos acima usariam 1241 em vez de 8834.

Solução de problemas do Nessus para Windows

Problemas de instalação/atualização

Problema: O log nessusd.messages indica que o nessusd foi iniciado, mas isto não ocorreu.

Solução: A mensagem “nesssud <version> started” indica apenas que o programa nessusd foi executado. A mensagem “nessusd is ready” (nessusd está pronto) indica que o servidor Nessus está em execução e pronto para aceitar conexões.

Problema: Estou recebendo o seguinte erro ao tentar instalar o Nessus Windows:

“1607: Unable to install InstallShield Scripting Runtime”

Solução: Este código de erro pode ser gerado se o serviço Windows Management Instrumentation (WMI) for desativado por qualquer motivo. Verifique se o serviço está sendo executado.

Se o serviço WMI estiver funcionando, pode ter ocorrido um problema entre as configurações do sistema operacional Microsoft Windows e o produto InstallShield usado para instalar e remover o Nessus Windows. Existem artigos nos bancos de dados de conhecimento da Microsoft e da InstallShield que explicam as possíveis causas e a resolução do problema.

- Artigo do banco de dados de conhecimento da Microsoft, ID 910816: http://support.microsoft.com/?scid=kb;en-us;910816
- Artigo do banco de dados de conhecimento da InstallShield ID Q108340: http://consumer.installshield.com/kb.asp?id=Q108340

Problemas de varredura

Problema: Não consigo realizar varreduras através da minha conexão PPP ou PPTP.

Solução: Atualmente, não há suporte para esta opção. Revisões futuras do Nessus Windows serão desenvolvidas com esta funcionalidade.

Problema: Uma verificação de vírus no sistema informa um grande número de vírus no Nessus Windows.

Solução: Alguns aplicativos antivírus podem reconhecer alguns dos plugins do Nessus como vírus. Exclua o diretório de plugins das varreduras de vírus, pois não há programas executáveis nesse diretório.

Problema: Estou realizando uma varredura em um dispositivo incomum, como um controlador RAID, e a varredura é interrompida porque o Nessus o detectou como uma impressora.

Solução: Desative “Safe Checks” (Verificações Seguras) na política de varredura antes da varredura do dispositivo. A varredura de uma impressora normalmente exige que a impressora seja reiniciada, portanto, quando “Safe Checks” (Verificações seguras) for ativado, os dispositivos detectados como impressoras não serão examinados.

Problema: Aparentemente, as varreduras de SYN não esperam até que a conexão com a porta seja estabelecida no Nessus Windows.

Solução: A varredura de SYN não estabelece uma conexão TCP completa, mas não altera os resultados da varredura.

Problema: Ao executar uma varredura, quais fatores afetam a velocidade ao executar o Nessus Windows em um sistema Windows XP?

Solução: A Microsoft fez alterações no Windows XP Service Pack 2 e 3 (Home e Pro), que podem afetar o desempenho do Nessus Windows e gerar falsos negativos. Atualmente, a pilha TCP/IP limita o número de tentativas de conexão TCP incompletas simultâneas de saída. Se o limite for atingido, as tentativas de conexão subsequentes serão colocadas em uma fila e serão atendidas a uma velocidade fixa (10 por segundo). Se houver muitas tentativas na fila, poderão ser descartadas. Consulte a página da Microsoft TechNet a seguir para obter mais informações:

http://technet.microsoft.com/en-us/library/bb457156.aspx

Isto faz com que uma varredura do Nessus no Windows XP gere falsos negativos, pois o XP permite apenas 10 conexões incompletas novas por segundo (no estado SYN). Para aumentar a precisão, recomenda-se que o ajuste de varredura de portas do Nessus em um sistema Windows XP seja limitado às configurações indicadas a seguir, encontradas nas configurações de varredura individuais para cada política de varredura:

Max number of hosts (Número máximo de hosts): 10
Max number of security checks (número máximo de verificações de segurança): 4

Para acelerar a varredura e torná-la mais confiável, é altamente recomendável que o Nessus Windows seja instalado em um produto de servidor da família Microsoft Windows, como o Windows Server 2003 ou Windows Server 2008.

Para obter mais informações

A Tenable Produziu vários outros documentos que detalham a instalação, a configuração, a operação pelo usuário e os testes gerais do Nessus. O documentos estão listados a seguir:

- **Guia do Usuário Nessus** – como configurar e operar a interface de usuário do Nessus.
- **Verificações de Credenciais do Nessus para Unix e Windows** – informações sobre como realizar varreduras autenticadas de rede com o scanner de vulnerabilidades Nessus,
- **Verificações de Conformidade do Nessus** – guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Referência de Verificações de Conformidade do Nessus** – guia completo da sintaxe das verificações de conformidade do Nessus.
- **Formato de arquivo Nessus v2** – descreve a estrutura do formato de arquivo `.nessus`, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Especificação do protocolo Nessus XML-RPC** – descreve o protocolo e a interface XML-RPC do Nessus.
- **Monitoramento de Conformidade em Tempo Real** – descreve como as soluções da Tenable podem ser usadas para ajuda a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.
- **Guia de administração SecurityCenter**

Outros recursos on-line são listados a seguir:

- Fórum de Discussão do Nessus: https://discussions.nessus.org/.
- Blog da Tenable: http://blog.tenable.com/
- Podcast da Tenable: http://blog.tenablesecurity.com/podcast/
- Vídeo de exemplos de uso: http://www.youtube.com/user/tenablesecurity
- Feed do twitter da Tenable: http://twitter.com/tenablesecurity

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço http://www.tenable.com/.

Declarações de licença de terceiros

Os pacotes de software de terceiros são disponibilizados pela Tenable para uso com o Nessus. Todos os componentes de terceiros com marcas de direitos autorais da Tenable estão sujeitos a outros termos de licença especificados na documentação.

Os plugins de terceiros são considerados “plugins de detecção de vulnerabilidades” conforme exemplificado a seguir.

A seção 1 (a) do Contrato de Licença do Nessus prevê:

Os plugins ou componentes sem as marcas de proteção por direitos autorais da Tenable não são plugins conforme definidos no âmbito do presente Contrato de Assinatura e estão sujeitos a outros termos de licença.

A Seção 1 (b) (i) do Contrato de Licença do Nessus prevê:

A assinatura inclui programas de detecção de vulnerabilidade não desenvolvidos pela Tenable ou por seus licenciados e que são licenciados a você nos termos de contratos separados. Os termos e as condições deste Contrato de Assinatura não se aplicam a esses programas de detecção de vulnerabilidades.

Partes do Software de Segurança de Rede da Tenable podem utilizar os seguintes materiais com direitos autorais, cuja utilização fica desde já reconhecida:

Partes Copyright (c) 1997-2008 Universidade de Cambridge (libpcre)

A redistribuição e o uso nos formatos “fonte” e “binário”, com ou sem modificação, são permitidos desde que as seguintes condições sejam cumpridas:

- As redistribuições do código-fonte devem manter o aviso de direitos autorais indicado acima, esta lista de condições e a isenção de responsabilidade.
- As redistribuições em forma binária devem reproduzir o aviso de direitos autorais acima, esta lista de condições e a isenção de responsabilidade, tanto na documentação como em outros materiais fornecidos com a distribuição.
- nome da Universidade de Cambridge, o nome da Google Inc. ou os nomes de seus colaboradores não podem ser mencionados para endossar ou promover produtos derivados deste software sem prévio consentimento por escrito.

ESTE SOFTWARE É FORNECIDO PELOS TITULARES DOS DIREITOS AUTORAIS E PELOS COLABORADORES "NO ESTADO EM QUE SE ENCONTRA" E NOS EXIMIMOS DE QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO E ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE. EM NENHUMA HIPÓTESE O TITULAR DOS DIREITOS AUTORAIS OU SEUS COLABORADORES SERÃO RESPONSÁVEIS PELOS DANOS INDIRETOS, INCIDENTAIS, ESPECIAIS E EXEMPLARES (INCLUSIVE, SEM LIMITAÇÃO A AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SUBSTITUTOS, IMPOSSIBILIDADE DE USO, PERDA DE DADOS OU LUCROS CESSANTES OU INTERRUPÇÃO DE NEGÓCIOS) CAUSADOS A QUALQUER TÍTULO SOB QUALQUER TEORIA DE RESPONSABILIDADE, SEJA POR FORÇA DE CONTRATO, RESPONSABILIDADE OBJETIVA OU ILÍCITO CIVIL (INCLUSIVE NEGLIGÊNCIA OU A OUTRO TÍTULO) DECORRENTE DE QUALQUER MANEIRA DO USO DO SOFTWARE, MESMO SOB ORIENTAÇÃO A RESPEITO DA POSSIBILIDADE DE TAIS DANOS.

Partes Copyright (c) 2000 The NetBSD Foundation, Inc. Todos os direitos reservados.

ESTE SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA PELA NETBSD FOUNDATION, INC. E PELOS COLABORADORES E NOS EXIMIMOS DE QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO E ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE. EM NENHUMA HIPÓTESE A FUNDAÇÃO OU SEUS COLABORADORES SERÃO

RESPONSÁVEIS PELOS DANOS INDIRETOS, INCIDENTAIS, ESPECIAIS E EXEMPLARES (INCLUSIVE SEM LIMITAÇÃO A AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SUBSTITUTOS, IMPOSSIBILIDADE DE USO, PERDA DE DADOS OU LUCROS CESSANTES OU INTERRUPÇÃO DE NEGÓCIOS) CAUSADOS A QUALQUER TÍTULO SOB QUALQUER TEORIA DE RESPONSABILIDADE, SEJA POR FORÇA DE CONTRATO, RESPONSABILIDADE OBJETIVA OU ILÍCITO CIVIL (INCLUSIVE NEGLIGÊNCIA OU A OUTRO TÍTULO) DECORRENTE DE QUALQUER MANEIRA DO USO DO SOFTWARE, MESMO SOB ORIENTAÇÃO A RESPEITO DA POSSIBILIDADE DE TAIS DANOS.

Partes Copyright (c) 1995-1999 Kungliga Tekniska Hogskolan (Instituto Técnico Real, Estocolmo, Suécia). Todos os direitos reservados.

ESTE SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA PELO INSTITUTO E PELOS COLABORADORES E NOS EXIMIMOS DE QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO E ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE. EM NENHUMA HIPÓTESE O INSTITUTO OU SEUS COLABORADORES SERÃO RESPONSÁVEIS PELOS DANOS INDIRETOS, INCIDENTAIS, ESPECIAIS E EXEMPLARES (INCLUSIVE SEM LIMITAÇÃO A AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SUBSTITUTOS, IMPOSSIBILIDADE DE USO, PERDA DE DADOS OU LUCROS CESSANTES OU INTERRUPÇÃO DE NEGÓCIOS) CAUSADOS A QUALQUER TÍTULO SOB QUALQUER TEORIA DE RESPONSABILIDADE, SEJA POR FORÇA DE CONTRATO, RESPONSABILIDADE OBJETIVA OU ILÍCITO CIVIL (INCLUSIVE NEGLIGÊNCIA OU A OUTRO TÍTULO) DECORRENTE DE QUALQUER MANEIRA DO USO DO SOFTWARE, MESMO SOB ORIENTAÇÃO A RESPEITO DA POSSIBILIDADE DE TAIS DANOS.

Partes Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd e Clark Cooper
Partes Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 mantenedores expatriados.

O SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA, SEM GARANTIAS DE NENHUMA ESPÉCIE, SEJAM ELAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E LEGALIDADE. EM NENHUMA HIPÓTESE OS AUTORES OU TITULARES DOS DIREITOS AUTORAIS SERÃO RESPONSÁVEIS POR QUAISQUER DEMANDAS, DANOS OU OUTRAS RESPONSABILIDADES, SEJA EM VIRTUDE DE AÇÃO JUDICIAL OU DO CONTRATO, OU A OUTRO TÍTULO, EM DECORRÊNCIA OU VIRTUDE DO SOFTWARE, DE SEU USO OU DE OUTRAS TRANSAÇÕES NO SOFTWARE.

Este produto contém software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit. (http://www.openssl.org/) Copyright (c) 1998-2007 The OpenSSL Project. Todos os direitos reservados.

ESTE SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA PELO OpenSSL PROJECT E PELOS COLABORADORES E NOS EXIMIMOS DE QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO E ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE. EM NENHUMA HIPÓTESE O OpenSSL PROJECT OU SEUS COLABORADORES SERÃO RESPONSÁVEIS PELOS DANOS INDIRETOS, INCIDENTAIS, ESPECIAIS E EXEMPLARES (INCLUINDO, SEM LIMITAÇÃO A AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SUBSTITUTOS, IMPOSSIBILIDADE DE USO, PERDA DE DADOS OU LUCROS CESSANTES OU INTERRUPÇÃO DE NEGÓCIOS) CAUSADOS A QUALQUER TÍTULO SOB QUALQUER TEORIA DE RESPONSABILIDADE, SEJA POR FORÇA DE CONTRATO, RESPONSABILIDADE OBJETIVA OU ILÍCITO CIVIL (INCLUSIVE NEGLIGÊNCIA OU A OUTRO TÍTULO) DECORRENTE DE QUALQUER MANEIRA DO USO DO SOFTWARE, MESMO SOB ORIENTAÇÃO A RESPEITO DA POSSIBILIDADE DE TAIS DANOS.

Partes Copyright (C) 1998-2003 Daniel Veillard. Todos os direitos reservados.

Fica desde já concedida a permissão, a título gratuito, a qualquer pessoa que obtenha uma cópia deste software e dos respectivos arquivos de documentação (o “Software”), para lidar com o Software sem restrições, inclusive, sem limitação, os direitos de usar, copiar, modificar, mesclar, publicar, distribuir, sublicenciar e/ou vender cópias do Software, e permitir que as pessoas a quem o Software seja fornecido o façam, sem prejuízo das seguintes condições:

O aviso de direitos autorais acima e este aviso de permissão devem ser incluídos em todas as cópias ou partes substanciais do Software.

O SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA, SEM GARANTIAS DE NENHUMA ESPÉCIE, SEJAM ELAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E LEGALIDADE. EM NENHUMA HIPÓTESE DANIEL VEILLARD SERÁ RESPONSÁVEL POR QUALQUER RECLAMAÇÃO, DANOS OU OUTRAS RESPONSABILIDADES, SEJA EM VIRTUDE DE AÇÃO JUDICIAL OU DO CONTRATO, OU A OUTRO TÍTULO, EM DECORRÊNCIA OU VIRTUDE DO SOFTWARE, DE SEU USO OU DE OUTRAS TRANSAÇÕES NO SOFTWARE.

Partes Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman e Daniel Veillard.
Todos os direitos reservados.

Fica desde já concedida a permissão, a título gratuito, a qualquer pessoa que obtenha uma cópia deste software e dos respectivos arquivos de documentação (o “Software”), para lidar com o Software sem restrições, inclusive, sem limitação, os direitos de usar, copiar, modificar, mesclar, publicar, distribuir, sublicenciar e/ou vender cópias do Software, e permitir que as pessoas a quem o Software seja fornecido o façam, sem prejuízo das seguintes condições:

O aviso de direitos autorais acima e este aviso de permissão devem ser incluídos em todas as cópias ou partes substanciais do Software.

O SOFTWARE É FORNECIDO NO ESTADO EM QUE SE ENCONTRA, SEM GARANTIAS DE NENHUMA ESPÉCIE, SEJAM ELAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE POSSIBILIDADE DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E LEGALIDADE. EM NENHUMA HIPÓTESE OS AUTORES SERÃO RESPONSÁVEIS POR QUALQUER RECLAMAÇÃO, DANOS OU OUTRAS RESPONSABILIDADES, SEJA EM VIRTUDE DE AÇÃO JUDICIAL OU DO CONTRATO, OU A OUTRO TÍTULO, EM DECORRÊNCIA OU VIRTUDE DO SOFTWARE, DE SEU USO OU DE OUTRAS TRANSAÇÕES NO SOFTWARE.

Sobre a Tenable Network Security

Tenable Network Security, líder em monitoramento unificado de segurança, é a criadora do scanner de vulnerabilidades Nessus e de soluções de primeira classe sem agente para o monitoramento contínuo de vulnerabilidades, pontos fracos de configuração, vazamento de dados, gerenciamento de logs e detecção de comprometimentos para ajudar a garantir a segurança da rede e o cumprimento das leis e normas FDCC, FISMA, SANS CSIS e PCI. Os produtos premiados da Tenable são utilizados por muitas organizações da Global 2000 e por órgãos públicos para tomar a iniciativa de reduzir os riscos nas redes. Para mais informações, visite http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

Copyright © 2013. Tenable Network Security, Inc. Todos os direitos reservados. Tenable Network Security e Nessus são marcas comerciais registradas da Tenable Network Security, Inc.